



Configuring the AccountCourier Access Request Manager™ Solution

Release 8.0

Courion Corporation

1900 West Park Drive
Westborough, MA 01581-3919
Phone: (508) 879-8400
Domestic Toll Free: 1-866-Courion
Fax: (508) 366-2844

Trademarks

Copyright (c) by Courion Corporation. All rights reserved. This document may be printed or copied for use by administrators of software that this guide accompanies. Printing or copying this document for any other purpose in whole or in part is prohibited without the prior written consent of Courion Corporation.

Courion[®], the Courion logo, AccountCourier[®], CertificateCourier[®], DIRECT![®], PasswordCourier[®], ProfileCourier[®], and RoleCourier[®] are all registered trademarks of Courion Corporation. Access Assurance Suite[™], AuditLink[™], ComplianceCourier[™], Dynamic Community[™], the ez Install logo, IdentityLnk[™], IdentityMap[™], Policy Publisher[™], PolicyLink[™], and ServiceLink[™] are trademarks of Courion Corporation.

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in technical Data and Computer Software clause in DFAR 52.227-7013 or the equivalent clause in FAR 52.227-19, whichever is applicable.

Courion Corporation reserves the right to make changes to this document and to the products described herein without notice. Courion Corporation has made all reasonable efforts to insure that the information contained within this document is accurate and complete. However, Courion Corporation shall not be held liable for technical or editorial errors or omissions, or for incidental, special, or consequential damages resulting from the use of this document or the information contained within it.

The names of additional products may be trademarks or registered trademarks of their respective owners. The following list is not intended to be comprehensive.

Adobe[®], the Adobe[®] logo, Acrobat[®], and Acrobat[®] Reader[®] are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

CA-TopSecret[®] and CA-ACF[®] are registered trademarks of Computer Associates International, Inc.

Citrix[®] is a registered trademark of Citrix Systems, Inc. in the United States and other countries.

HP-UX is an X/Open[®] Company UNIX[®] branded product.

Java[™] and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Microsoft Corporation[®], Microsoft Windows[®], Microsoft Windows NT[®], Microsoft Excel[®], Microsoft Access[™], Microsoft Internet Explorer[®], and SQL Server[®] are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Microsoft is a U.S. registered trademark of Microsoft Corp.

Netscape[®] is a registered trademark of Netscape Communications Corporation[®] in the U.S. and other countries. Netscape Communicator[®], Netscape Navigator[®], and Netscape Directory Server[®] are also trademarks of Netscape Communications Corporation and may be registered outside of the U.S.

Novell[®] and the Novell products, including NetWare[®], NDS[®], GroupWise[®], and IntraNetWare[®] are all registered trademarks of Novell.

IBM[®], Lotus[®], Lotus Notes[®], Domino[®], i5/OS[®], z/OS[®], and RACF are registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Oracle[®] and PeopleSoft[®] are registered trademarks of the Oracle Corporation. Oracle8[™] and Oracle9[™] are trademarks of the Oracle Corporation.

Remedy[®], Action Request System[®], and AR System[®] are registered trademarks of BMC Software, Inc.

SAP, the SAP logo, mySAP.com, and R/3 are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.

SecurID[®] and BSAFE[®] are registered trademarks of RSA Security Inc. All rights reserved.

Sun, Sun Microsystems, the Sun Logo, iPlanet are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the United States and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Copyright to STLport is owned by the following entities: Boris Fomitchev[®] (1999/2000), Hewlett-Packard Company[®] (1994), Silicon Graphics Computer Systems, Inc.[®] (1996/1997), and the Moscow Center for SPARC Technology[®] (1997).

All other products and companies mentioned in this document may be the trademarks of their associated organizations.

June 2011

Contents

Chapter 1 - About the Access Request Manager	5
Access Keys	6
Chapter 2 - About The Access Request Manager Workflows	7
Making a Request	8
Approving a Request	11
Chapter 3 - Overview of the Administration Interface	13
Installing and Configuring the Access Request Manager	14
Before Installation Configuration	14
After Installation Configuration	14
Adding Connection Strings	14
Executing SQL Scripts	15
Configuring the Courion Request Service	16
Configuring the Courion Notification Service	16
Accessing the Administration Interface	18
Using the Top-Level Menu Options for the Administration Interface	18
The Application/Accesses Menu Item	19
The Configuration Menu Item	19
The Security Admin Menu Item	19
The Priority Disable Menu Item	20
The Admin - View All Requests Menu Item	20
Using the Global Configuration Manager	21
Default Global Options	21
Editing Global Options	29
Editing Global Options with Config Type as Text	30
Editing Global Options with Config Type as Complex	30
Specifying Custom Macros in the Edit Complex Value Editor	32
Using the Pick List Admin	34
Default Picklist Types and Values	35
Adding a PickList Value	36
Chapter 4 - Configuring the Access Request Workflow	39
Selecting Recipients	40
Specifying Categories for the Providing Access For Drop-Down List	40
Displaying Radio Buttons for Searching or Adding New Recipients	41
Setting Up the Search to Look for Recipients	41
Specifying the Unique Search by Field	42
Specifying Fields for More Search Options	42
Displaying the Search Results	42
Displaying the Result for Search by Field	43
Displaying the Results for More Search Options	43
Displaying the Checkbox with More Search Options Results	43
Configuring fields to Add a New Recipient	44
Constraining the Search Options for Requesters	44
Custom Macros to Implement Default Search Restrictions	45
Custom Macros to Retrieve User Information	46
Selecting Access Levels	47
Configuring the Primary and Secondary Drop-Down Lists	47
Adding Applications	48
Adding Access Levels	50
Adding Target Attributes	51

Adding Roles	55
Configuring the Access Level Fields Displayed to the Requester	58
Configuring the Confirmation Popup	58
Constraining the Access Levels Visible to Requesters	58
Custom Macros to Implement for Adding Access Levels	59
Verifying Access Levels	60
Chapter 5 - Configuring the Approval Workflow	61
Adding Second-Level Approvers	62
Approving the Requests	64
Setting Up Fields for Pending Requests	64
Setting Up Fields for Request Details	64
Setting Up Fields To View Requester Details	65
Setting Up Fields to View Recipient Details	65
Setting Up Fields to View Access Levels	65
Configuring the Approve and Deny Action Buttons	66
Displaying the Checkbox to Enable Collective Approval	66
Displaying the Checkbox to Enable Only Collective Approval	67
.....	67
Chapter 6 - Setting Up Email Notifications	69
Editing a Default Email Template	70
Chapter 7 - Managing Access to the Access Request Manager Web Pages	73
Community	74
Entitlements	75
Securing Access to Web Pages	76
Entitlement and Web Page Pairs in the Access Request Manager	77
Adding Web Pages for a New Entitlement	78
Changing the Default Landing Page of the Portal	78
Functions	79
Chapter 8 - Customizing the Access Request Manager User Interface	81
Displayed Text in the Resource File	81
Chapter 9 - Disabling Access with Priority Disable	87
Index	89

Chapter 1: About the Access Request Manager

The AccountCourier Access Request Manager™ Solution is a component of the Access Assurance Suite that resides within the Access Assurance Portal. The Access Request Manager is a complete, highly functional request management system that enables:

- An individual, whether in IT or in a line of business, to request access to resources, such as an online application system.
- Designated approvers to approve or reject requests.

The Access Request Manager is designed for users with distinct functions within an enterprise, including:

- **Individual Contributors** - request access for themselves and for others if entitled by enterprise policy,
- **Business Managers** - request access for themselves, request access for direct reports and, if entitled by the enterprise policy, for others. They can also approve requests for their direct reports if authorized by the enterprise policy.

Business Managers are users who have direct reports.

- **Resource Owners** - request access for themselves or others, and approve access to resources for which they are responsible.

Resource Owners are users who own IT resources.

This manual is intended for use by an IT administrator who can configure the Access Request Manager. It describes how to use the Access Request Manager Administration Interface available through the Access Assurance Portal to configure the request and approval workflows, and includes the following chapters:

- [“About The Access Request Manager Workflows” on page 7](#) describes the request and the approval workflows, and the windows associated with it.
- [“Overview of the Administration Interface” on page 13](#) describes how to access the Administration Interface through the Access Assurance Portal to configure the request and approval workflows.
- [“Configuring the Access Request Workflow” on page 39](#) describes how to configure the User Detail, the Access Catalog and the Verify windows for the request workflow.
- [“Configuring the Approval Workflow” on page 61](#) describes how to configure approvers and the Request Approval window for the approval workflow.
- [“Setting Up Email Notifications” on page 69](#) describes how to create and maintain email templates for notifications sent to requesters, recipients, and approvers.
- [“Managing Access to the Access Request Manager Web Pages” on page 73](#) describes how to configure users to see only those web pages they are entitled to in the Access Request Manager.
- [“Customizing the Access Request Manager User Interface” on page 81](#) describes how to customize the text for buttons, tabs, and dialog boxes.

- [“Disabling Access with Priority Disable” on page 87](#) describes how to disable access for a terminated user.

Access Keys

The Access Request Manager requires an access key, obtained from Courion. If you use roles with the Access Request Manager, this also requires an access key, obtained from Courion.

Chapter 2: About The Access Request Manager Workflows

This chapter describes the Access Request Manager workflows and the windows you have to configure to enable them.

The Access Request Manager includes the following workflows, which enable users to request and approve access seamlessly:

- **The request workflow** - The steps the requester completes to make a request to IT resources in an enterprise. This workflow involves selecting recipients, selecting access levels and finally verifying all the information. [“Making a Request” on page 8](#) provides more information about this workflow.

Requesters are users who request access for themselves or others. By default, this includes Individual Contributors, Business Managers and Resource Owners. A recipient includes any person in an enterprise who is given access to an IT resource.

- **The approval workflow** - The steps the approver completes to approve outstanding requests. [“Approving a Request” on page 11](#) includes more information about this workflow.

Approvers are users who approve requests. Typically, Business Managers and Resource Owners are approvers.

Making a Request

To access the Access Request Manager, a requester authenticates through the Access Assurance Portal. Upon authentication, the Access Request Manager is available, as shown in [Figure 1](#).

Note: The Access Request Manager top-level menu items are **ACCESS REQUEST**, **REQUEST APPROVAL**, **VIEW REQUEST**, **PRIORITY DISABLE** and the Administration Interface menu options. Depending on the function of the user who logs in to the Access Request Manager, a top-level menu relevant to that user appears. For example, a Business Manager sees **ACCESS REQUEST**, **VIEW REQUEST**, and **REQUEST APPROVAL**.

Selecting **ACCESS REQUEST** presents the tabs **USER DETAIL**, **ACCESS CATALOG** and **VERIFY**.

Figure 1: Access Request Manager with the User Detail Window

On the **USER DETAIL** window, the requester follows these steps to make a request:

1. **Selects recipients:** Requesters can select one or more recipients on the **USER DETAIL** window. If they select more than one recipient, the same access levels will be requested for all recipients.

Depending on their function in the enterprise, requesters can request access for themselves or other recipients. By default:

- Individual Contributors can only select themselves.
Note: Users who are neither Business Managers nor Resource Owners are Individual Contributors.
- Business Managers can select themselves or their direct reports.
Note: The user is a Business Manager if the Business Manager's ProfileUID appears in the ManagerID field of others in the Profile table. For example, if the Business Manager, David Larson, has a direct report called Jack Smith, then David Larson's ProfileUID appears in the ManagerID field for Jack Smith.
- Resource Owners can select themselves or any other recipients.
Note: The user is a Resource Owner if the Resource Owner's ProfileUID appears in the Owner field of the Application table.

If requesters are requesting access for themselves, the search options appear with their profile information. If requesters want to request access for other recipients, they are presented with search options that allow them to search by a unique field or use broader criteria to search for one or more recipients. The requester can add a new recipient if no recipient was found using the search options.

Items that you can configure on the **USER DETAIL** window, for example:

- Radio buttons for searching or adding new recipients.
- Search fields by which a requester searches for recipients.
- The option to add a new recipient if no recipients are found using the search options.

To configure the **USER DETAIL** window, refer to the section [“Selecting Recipients” on page 40](#).

The requester proceeds to the **ACCESS CATALOG** window to add access levels.

2. **Selects access levels:** Requesters select one or more access levels for the recipients on the **ACCESS CATALOG** window, as shown in [Figure 2](#).

Note: Access levels are a set of entitlements, or permissions, for an IT resource. The entitlements are grouped so that the user sees a business-friendly resource name.

Figure 2: Access Request Manager with the Access Catalog Window

The screenshot shows the 'Access Catalog' window in the Access Request Manager. At the top, there are navigation tabs: 'Portal Home', 'Access Request', 'View Requests', and 'Request Approval'. Below these are sub-tabs: 'User Detail', 'Access Catalog', and 'Verify'. The main content area includes:

- Filter By:** A dropdown menu set to 'Applications'.
- Applications:** A dropdown menu set to 'Kronos Workforce Timekeeper'.
- Filter Results:** A table with columns 'Application Name', 'Access', 'Add', and 'Info'. It lists three entries for 'Kronos Workforce Timekeeper' with access levels 'WFC TK admin', 'WFC TK exempt', and 'WFC TK non-exmpt'.
- Selected Employees:** A table with columns 'FirstName', 'LastName', 'Location', 'Department', and 'StartDate'. It shows one employee: John Smith, Westborough, Sales.

At the bottom right, there are 'Back' and 'Next' buttons. A copyright notice at the very bottom reads: 'Copyright © Courion Corporation. All rights reserved.'

Depending on their function in the enterprise, requesters can see only those access levels relevant to them. By default:

- Individual Contributors see all access levels.
- Business Managers see all access levels.
- Resource Owners see only access levels for resources they own.

Note: Resource Owners who are also Business Managers see all access levels if they selected only their direct reports on the **USER DETAIL** window.

For additional information about which access levels requesters can see, refer to [“Functions” on page 79](#).

Requesters can provide configuration information for access levels, as needed, such as the dollar amount for check approval authority. Items that you can configure on the **ACCESS CATALOG** window, for example:

- Filters for requesters so that they can select relevant access levels.
- The entitlements that comprise the access levels, which a requester can select.

To configure the **ACCESS CATALOG** window, refer to the section [“Selecting Access Levels” on page 47.](#)

3. Verifies the selected access levels: Requesters verify the access levels on the **VERIFY** window selected by them on **ACCESS CATALOG**, as shown in [Figure 3.](#) Requesters can update any configuration information before submitting the request for approval. Requesters can also modify or remove any access levels approved earlier through the Access Request Manager.

Note: No approval is required for an access level that is being removed.

Figure 3: Access Request Manager with the Verify Window

Portal Home Access Request View Requests Request Approval

User Detail Access Catalog Verify

Remove Selected

Application Name	Action	Access	User: Conf
Kronos Workforce Timekeeper	Added	WFC TK exempt	

Selected Employees

FirstName	LastName	Location	Department	StartDate
John	Smith	Westborough	Sales	

Back Submit

Copyright © Courion Corporation. All rights reserved.

Items that you can configure on the **VERIFY** window include:

- Fields to show the user access information on the popup.

To configure the **VERIFY** window, refer to the section [“Verifying Access Levels” on page 60.](#)

An email notification is sent to the requester, recipient, and the approver about the request. To configure the email notifications, refer to [“Setting Up Email Notifications” on page 69.](#)

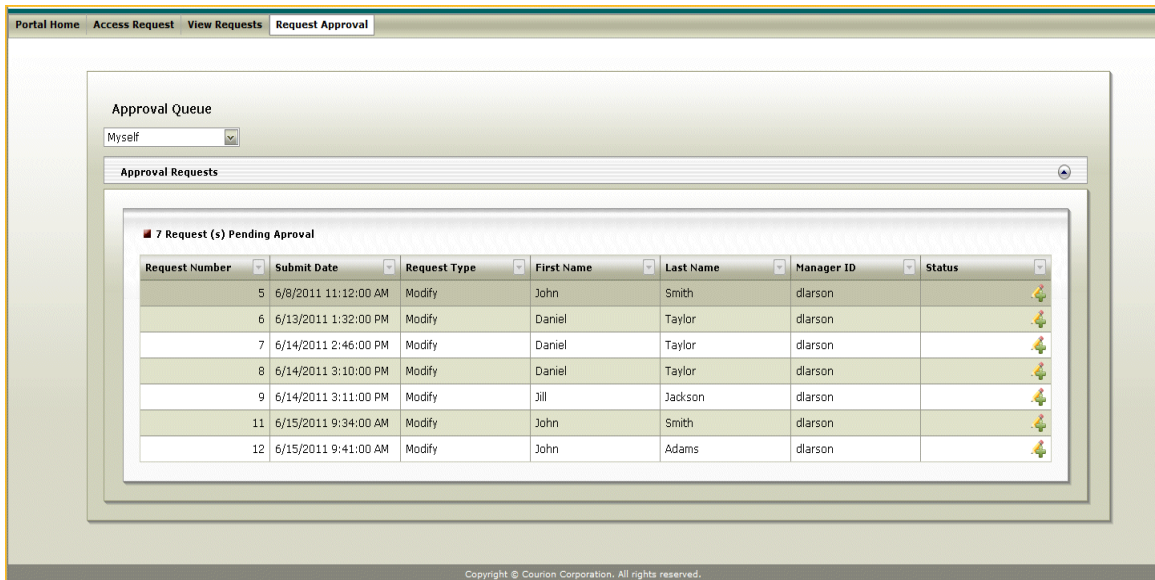
Approving a Request

When approvers access the Access Request Manager, they see the **REQUEST APPROVAL** menu item.

On selecting **REQUEST APPROVAL**, approvers see their outstanding requests to approve, as shown in [Figure 4](#).

If a request was submitted as a bulk request (a request with more than one recipient), it is separated into multiple requests on **REQUEST APPROVAL** with one request for each recipient. For example, a bulk request that includes three recipients with two access levels splits into three separate requests on **REQUEST APPROVAL**. Each request includes one recipient and two access levels. Splitting the bulk request enables the approver to act independently on each access level for each recipient.

Figure 4: Access Request Manager with the Request Approval



You can configure whether approvers can do a collective approval of requests, that is, for all items on the request. Depending on the enterprise policy, approvers could be required to approve each access level individually, or be allowed to approve all access levels in one action.

Refer to [“Configuring the Approval Workflow” on page 61](#) for adding approvers and configuring the **REQUEST APPROVAL** window.

Chapter 3: Overview of the Administration Interface

This chapter describes how to install and configure the Access Request Manager. It also describes how to use the Administration Interface to configure the request and approval workflows. This chapter includes the following sections:

- [*"Installing and Configuring the Access Request Manager" on page 14*](#)
- [*"Accessing the Administration Interface" on page 18*](#)
- [*"Using the Global Configuration Manager" on page 21*](#)
- [*"Using the Pick List Admin" on page 34*](#)

Installing and Configuring the Access Request Manager

The Access Request Manager is installed with the Access Assurance Suite as described in the manual *Installing the Access Assurance Suite*.

Before Installation Configuration

1. Populate the IdentityMap and Profile tables first before you install the Access Request Manager.
2. Configure the following:
 - An Active Directory domain with the Active Directory groups, including **Business Managers, Resource Owners, Access Approvers** and **ARM Admins**.

Note: A user with direct reports belongs to the Business Manager Active Directory group.

- An Active Directory target named **Active Directory**.
- A Microsoft-ADO-3.0 target named **Transaction Repository**. This target should point to the Transaction Repository database or where the schema for the Access Assurance Portal resides.
- A Microsoft-ADO-3.0 target named **ARM**. This target should point to the Access Request Manager database.

See *Configuring Password Management Modules (PMMs), Connectors, and Agents* for information on how to create the targets.

After Installation Configuration

After you install the Access Request Manager:

- Add connection strings.
- Execute SQL scripts to create, for example, tables, views, and stored procedures.
- Configure the Courion request service
- Configure the Courion notification service

Adding Connection Strings

Add the following Connection Strings:

- MetricRepositoryDefault and Default connection strings in the Analytics\AccessCertification\Web.Config file. The connection strings should point to the schema which has the 8.0 Transaction Repository installed.

```
<!--<add name="MetricRepositoryDefault"
connectionString="Data Source= $$YOURSERVERHERE$$;Initial
Catalog= $$YOURDBHERE$$;Trusted_Connection=True"
providerName="System.Data.SqlClient" />-->
```

```
<!--<add name="Default" connectionString="Data
Source= $$YOURSERVERHERE$$;Initial
Catalog= $$YOURDBHERE$$;Trusted_Connection=True"
providerName="System.Data.SqlClient" />-->
```

- MetricRepositoryDefault, dbConnectionString, and ARMEntities in the Analytics\AccessRequest\Web.Config file. The MetricRepositoryDefault connection string should point to the schema which has the 8.0 Transaction Repository installed. The dbConnectionString and ARMEntities should point to the ARM database.

```
<!--<add name="MetricRepositoryDefault"
connectionString="Data Source= $$YOURSERVERHERE$$;Initial
Catalog= $$YOURDBHERE$$;Trusted_Connection=True"
providerName="System.Data.SqlClient" />-->
    <!--<add name="dbConnectionString"
connectionString="Data Source= $$YOURSERVERHERE$$;Initial
Catalog= $$YOURDBHERE$$;Trusted_Connection=True"
providerName="System.Data.SqlClient" />-->
<!--<add name="ARMEntities" connectionString="metadata=res:/
/*;provider=System.Data.SqlClient;provider connection
string=&quot;Data Source= $$YOURSERVERHERE$$;Initial
Catalog= $$YOURDBHERE$$;Trusted_Connection=True;MultipleActiv
eResultSets=True&quot;"
providerName="System.Data.EntityClient" />-->
```

Executing SQL Scripts

Execute the following SQL scripts for the Access Request Manager available in the given location:

C:\Program Files (x86)\Courion Corporation\Analytics\AccessRequest\SQL

- access request database.sql - installs the ARM schema on a Microsoft SQL Server version supported by the Access Request Manager. Run this script first so that the schema creates all of the tables, views and stored procedures relevant to the Access Request Manager.
- emailtemplates-data.sql - creates the default email templates.
- globalconfigvalues-data.sql - generates the default global options.
- picklist-data.sql - generates the default picklists.
- workflows-data.sql - populates the Workflow table with the Access Request Manager workflow information.
- entitlement-page mapping.sql - adds default entitlements to the SecurityGroup table. The SQL script secures web page access by mapping the default entitlements to the relevant web pages in the SecurityPages table.
- portal menu.sql - configures the Access Assurance Portal menu and populates the Portal Menu table. Execute this script on the Transaction Repository database, or from the location that the connection string MetricRepositoryDefault points to in the Courion-installation-folder\Analytics\AccessRequest\Web.Config file.

Note: Execute all the scripts, except portal menu.sql, from the same location where the ARM schema resides, or from the location that the connection string dbConnectionString points to in the Courion-installation-folder\Analytics\AccessRequest\Web.Config file.

Configuring the Courion Request Service

Add the configuration for the request service to the Courion.Framework.RequestService.exe.config file found in the [courion-installation-folder]\CourionService folder. The request service processes the automated and manual requests on which approvers have taken action. The configuration file contains the following information:

```
<configuration>
  <appSettings>
    <add key="CourionServer" value="http://localhost/
courion/WebSamples/AccessOptions/XMLAO/xmlao.asp" />
    <add key="NumberToProcess" value="5" />
    <add key="SleepTime" value="1" />
    <add key="AppName" value="Courion Request Service" />
    <add key="ManualProcedure"
value="rs_ProcessManualRequests" />
  </appSettings>
  <connectionStrings>
    <!--<add name="dbConnectionString"
connectionString="Data Source= $$YOURSERVERHERE$$;Initial
Catalog= $$DatabaseName$$;User
ID= $$UserID$$;Password= $$Password$$ "
providerName="System.Data.SqlClient" />-->
  </connectionStrings>
</configuration>
```

CourionServer: The link to the XMLAO processing engine where the Courion Server is hosted.

NumberToProcess: The number of requests to process.

SleepTime: The number of minutes the service goes to sleep after processing the number of requests specified in NumberToProcess.

AppName: The name of the service.

ManualProcedure: The default rs_ProcessManualRequests stored procedure processes the manual requests.

dbConnectionString: The connection string points to the database which holds the ARM schema.

The courrequestservice.log log file for the request service is found in the [courion-installation-folder]\CourionService folder. It logs errors, warnings or any information related to the request service.

Configuring the Courion Notification Service

Add the configuration for the notification service to the Courion.Framework.NotificationService.exe.config file found in the [courion-installation-folder]\CourionService folder. The notification service sends notification when an event occurs, such as a request is submitted, approved or denied. The configuration file contains the following information:

```
<configuration>
```



```

<appSettings>
  <add key="SMTPServer" value="" />
  <add key="SenderAddress" value="" />
  <add key="SleepTime" value="1" />
  <add key="EnableLogging" value="true" />
  <add key="AppName" value="Courion Notification Service" /
>
  <add key="UserName" value="" />
  <add key="Password" value="" />
  <!--<add key="LogLevel" value="" />-->
</appSettings>
<connectionStrings>
  <!--<add name="dbConnectionString"
connectionString="Data Source= $$YOURSERVERHERE$$;Initial
Catalog= $$DatabaseName$$;User
ID= $$UserID$$;Password= $$Password$$ "
providerName="System.Data.SqlClient" />-->
</connectionStrings>
</configuration>

```

SMTPServer: The server that sends emails.

SenderAddress: The email address from which emails are sent to requesters, approvers and administrators.

SleepTime: The number of minutes the service goes to sleep after processing pending notifications.

EnableLogging: Not applicable; however, do not remove.

AppName: The name of the service.

UserName: The administrative account for the SMTP server.

Password: The administrative account password for SMTP Server.

LogLevel: Log level can be classified into different levels with 0 for error, 1 for warning and error, 2 for information, warning and error.

The cournotificationservice.log log file for the notification service is found in the [courion-installation-folder]\CourionService folder. It logs errors, warnings or any information related to the notification service.

Accessing the Administration Interface

The Administration Interface for the Access Request Manager is available through the Access Assurance Portal. To access the Administration Interface you have to be a member of the ARM Admins Active Directory group.

To access the Portal on the server where it is installed, navigate to:

`http://localhost/analytics/accesscertification/login.aspx`

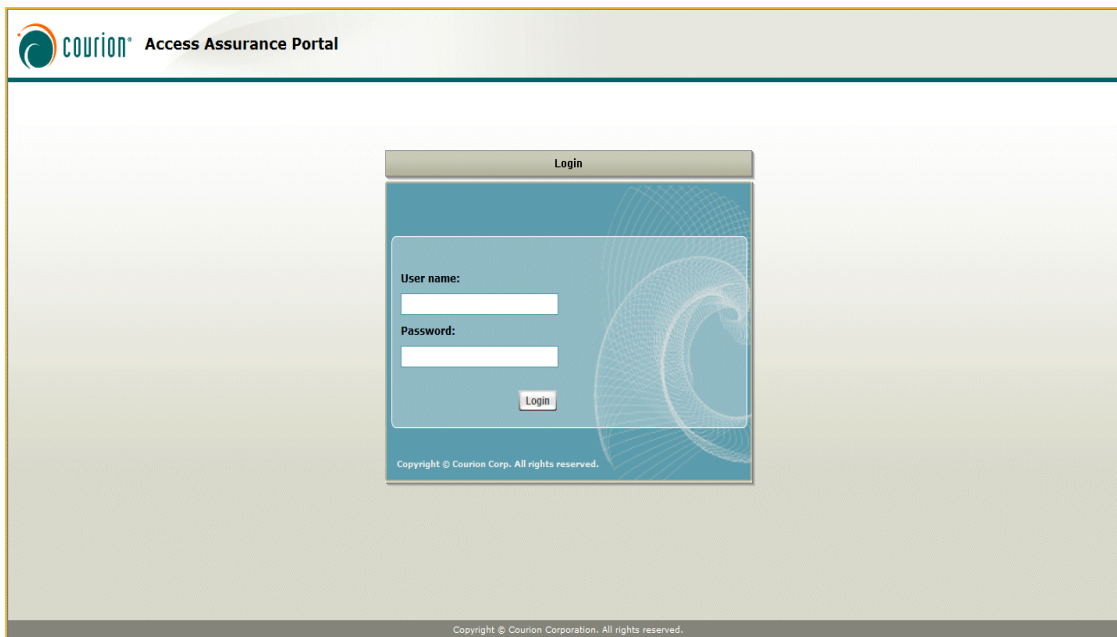
To access the Portal from another system, navigate to:

`http://[machine-name or IP Address]/analytics/accesscertification/login.aspx`

The window in [Figure 5](#) appears for you to authenticate in to the Access Assurance Portal.

Note: If the Integrated Windows Authentication feature is configured, you are automatically authenticated in to the Access Assurance Portal.

Figure 5: The Access Assurance Portal



Using the Top-Level Menu Options for the Administration Interface

Upon authentication, the top-level menu items of the Administration Interface are available to start configuring the request and approval workflows, as shown in [Figure 6](#).

Figure 6: The Administration Menu

The Application/Accesses Menu Item

APPLICATION/ACCESSES - Configure access levels for applications, such as Microsoft Active Directory, and add target attributes for the request workflow through the **APPLICATION/ACCESS MANAGER**. For more information, refer to the chapter [“Configuring the Access Request Workflow” on page 39](#).

To add approvers for the approval workflow through the **APPLICATIONS/ACCESS MANAGER**, refer to the chapter [“Configuring the Approval Workflow” on page 61](#).

The Configuration Menu Item

Selecting **CONFIGURATION** presents a submenu that includes:

- **GLOBAL CONFIGURATION MANAGER** - Use the **GLOBAL CONFIGURATION MANAGER** to configure the global options for the request and approval workflows. See [“Using the Global Configuration Manager” on page 21](#).
- **PICK LIST CONFIGURATION** - Access the **PICK LIST ADMIN** to create and manage picklists. See [“Using the Pick List Admin” on page 34](#) for more details on picklists.
- **EMAIL TEMPLATE CONFIGURATION** - Access the **EMAIL TEMPLATES MANAGER** to configure the email notifications sent to requesters, recipients, and approvers. Refer to the chapter [“Setting Up Email Notifications” on page 69](#) for additional information.
- **ROLES/ACCESS MAPPING** - Select **ROLES** to access the **ROLE MANAGER**, and add a new role. For example, add a new role such as QA Engineer, and map existing access levels to this role. For more information, refer to the chapter [“Configuring the Access Request Workflow” on page 39](#).

The Security Admin Menu Item

Select **SECURITY ADMIN** to configure which Active Directory Groups have access to which web pages in the Access Request Manager. For more information, refer to the chapter [“Managing Access to the Access Request Manager Web Pages” on page 73](#).

The Priority Disable Menu Item

Select **PRIORITY DISABLE** to disable access for a terminated user. For more information, refer to the chapter [“Disabling Access with Priority Disable” on page 87](#).

The Admin - View All Requests Menu Item

Select **ADMIN - VIEW ALL REQUESTS** to view all the pending requests. There are no options to configure on this window.

Using the Global Configuration Manager

The **GLOBAL CONFIGURATION MANAGER** appears when you select **CONFIGURATION > GLOBAL CONFIGURATION MANAGER**. It enables you to configure global options for the request and approval workflows to manage and optimize the Access Request Manager. The global options that you can configure include fields to display for search results or add new recipients, constraints to implement, or fields to display for requests.

This section lists the default global options that are configurable, and describes the general procedure to edit them. For specific details about the global options and how they affect the Access Request Manager workflows, refer to the individual chapters.

Default Global Options

Table 1 lists all the default global options with a brief description about what each does.

Table 1: The Default Global Options

Global Option (CONFIG NAME)	Description	Default (CONFIG VALUE)	More Information
AccessCatalogDefault RestrictionMacro	<p>Calls the macro that defines the restrictions on the display of access levels on the ACCESS CATALOG window.</p> <p>Accepts a custom macro name.</p> <p>CONFIG TYPE: Text.</p>	Get AccessCatalog Default Restriction	<p>“Constraining the Access Levels Visible to Requesters” on page 58</p> <p>For more information about the custom macro the global option references, see “Custom Macros to Implement for Adding Access Levels” on page 59.</p>
AccessCatalogFields	<p>Used to configure the fields for the FILTER RESULTS grid for access levels on the ACCESS CATALOG window.</p> <p>The field names specified in the XML string are from the AccessCatalogView.</p> <p>CONFIG TYPE: Complex.</p>		<p>“Configuring the Access Level Fields Displayed to the Requester” on page 58</p>

Table 1: The Default Global Options

Global Option (CONFIG NAME)	Description	Default (CONFIG VALUE)	More Information
AccessCatalogFilters	<p>Provides the contents for the primary and secondary drop-down lists on the ACCESS CATALOG window.</p> <p>The fields are from the AccessCatalogView.</p> <p>CONFIG TYPE: Complex.</p>	<p>If Applications is selected in the primary drop-down list, names of applications appear in the secondary drop-down list.</p> <p>If Roles is selected in the primary drop-down list, all the roles appear in the secondary drop-down list.</p> <p>For Ad Hoc, no secondary drop-down list is populated since all the access levels are displayed.</p>	<p>“Configuring the Primary and Secondary Drop-Down Lists” on page 47</p>
AccessCatalogIndividualContributorRestrictionMacro	<p>Calls the macro that defines the restrictions on the ACCESS CATALOG window for an Individual Contributor.</p> <p>Accepts a custom macro name.</p> <p>CONFIG TYPE: Text.</p>	Get AccessCatalog Individual Contributor Restriction	<p>“Constraining the Access Levels Visible to Requesters” on page 58</p> <p>For more information about the custom macro the global option references, see “Custom Macros to Implement for Adding Access Levels” on page 59.</p>
AccessCatalogManagerRestrictionMacro	<p>Calls the macro that defines the restrictions on the ACCESS CATALOG window for a Business Manager.</p> <p>Accepts a custom macro name.</p> <p>CONFIG TYPE: Text.</p>	Get AccessCatalog Manager Restriction	<p>“Constraining the Access Levels Visible to Requesters” on page 58.</p> <p>For more information about the custom macro the global option references, see “Custom Macros to Implement for Adding Access Levels” on page 59.</p>

Table 1: The Default Global Options

Global Option (CONFIG NAME)	Description	Default (CONFIG VALUE)	More Information
AccessCatalogResource OwnerRestrictionMacro	<p>Calls the macro that defines the restrictions on the ACCESS CATALOG window for a Resource Owner.</p> <p>Accepts a custom macro name.</p> <p>CONFIG TYPE: Text.</p>	Get AccessCatalog Resource Owner Restriction	<p>“Constraining the Access Levels Visible to Requesters” on page 58.</p> <p>For more information about the custom macro the global option references, see “Custom Macros to Implement for Adding Access Levels” on page 59.</p>
AccessCatalogShow ConfirmationPopup	<p>If true, displays a popup for requesters to confirm the access levels they have selected.</p> <p>CONFIG TYPE: Text. Enter true or false.</p>	True	<p>“Configuring the Confirmation Popup” on page 58</p>
AccessCatalogView	<p>The view referenced here provides information for the global options AccessCatalogFields and AccessCatalog Filters.</p> <p>To customize the view, modify AccessCatalogview or create a new view.</p> <p>CONFIG TYPE: Text. Accepts the name of the view.</p>	AccessCatalogView By default, the view joins the various application, access level and role related tables.	
AddNewAssigneeFields	<p>Used to configure the fields for the ADD NEW grid on the USER DETAIL window to add a new recipient.</p> <p>The fields are from the Profile table.</p> <p>CONFIG TYPE: Complex.</p>		<p>“Configuring fields to Add a New Recipient” on page 44.</p>

Table 1: The Default Global Options

Global Option (CONFIG NAME)	Description	Default (CONFIG VALUE)	More Information
ApprovalAccessDisplay Fields	Used to configure the fields for the ACCESS grid on the REQUEST DETAILS window. The fields are from the RequestApprovals table. CONFIG TYPE: Complex.		“Setting Up Fields to View Access Levels” on page 65
ApprovalActionApprove	Used to configure the APPROVE button in the APPROVAL REQUEST grid on the REQUEST APPROVAL window. CONFIG TYPE: Complex.	Displays the Approve action button.	“Configuring the Approve and Deny Action Buttons” on page 66
ApprovalActionDeny	Used to configure the DENY button in the APPROVAL REQUEST grid on the REQUEST APPROVAL window. CONFIG TYPE: Complex.	Displays the Deny action button. Requires a comment from the approver.	“Configuring the Approve and Deny Action Buttons” on page 66
ApprovalBulkActionOnly	Used to configure the SELECT ALL checkbox in the Access grid on the REQUEST DETAILS window. This global option only enables collective approval when set to True. Checkboxes to perform individual approvals on requests are not available. Enter true or false. CONFIG TYPE: Text.	False	“Displaying the Checkbox to Enable Only Collective Approval” on page 67

Table 1: The Default Global Options

Global Option (CONFIG NAME)	Description	Default (CONFIG VALUE)	More Information
ApprovalBulkAction Available	<p>Used to configure the SELECT ALL checkbox in the Access grid on the REQUEST DETAILS window. It enables the approver to do collective approval of requests if set to True. Checkboxes to perform individual approvals of requests remain available.</p> <p>Enter true or false.</p> <p>CONFIG TYPE: Text.</p>	True	“Displaying the Checkbox to Enable Collective Approval” on page 66
ApprovalProfileDisplay Fields	<p>Used to configure the fields for the EMPLOYEE grid on the REQUEST DETAILS window.</p> <p>The fields are from the Profile table.</p> <p>CONFIG TYPE: Complex.</p>		“Setting Up Fields to View Recipient Details” on page 65
ApprovalQueueDisplay Columns	<p>Used to configure the fields for the APPROVAL REQUESTS grid on the REQUEST APPROVAL window.</p> <p>The fields are from the Request table.</p> <p>CONFIG TYPE: Complex.</p>		“Setting Up Fields for Pending Requests” on page 64
ApprovalRequestDetail Fields	<p>Used to configure fields for the REQUEST grid on the REQUEST DETAILS window.</p> <p>The fields are from the Request Detail table.</p> <p>CONFIG TYPE: Complex.</p>		“Setting Up Fields To View Requester Details” on page 65

Table 1: The Default Global Options

Global Option (CONFIG NAME)	Description	Default (CONFIG VALUE)	More Information
LoggedInUserNameMacro	<p>Calls the macro that retrieves the name of the logged in requester, approver or the administrator.</p> <p>Accepts a custom macro name.</p> <p>CONFIG TYPE: Text.</p>	Get LoggedInUser Name	For more information about the custom macro the global option references, see “Custom Macros to Retrieve User Information” on page 46.
LoggedInUserRoleMacro	<p>Calls the macro that retrieves the function of the logged in user, such as a Resource Owner.</p> <p>Accepts a custom macro name.</p> <p>CONFIG TYPE: Text.</p>	Get LoggedInUser Role	For more information about the custom macro the global option references, see “Custom Macros to Retrieve User Information” on page 46.
MultiUserSearch Restriction	<p>Used to show or hide the checkbox with MORE SEARCH OPTIONS on the USER DETAIL window.</p> <p>CONFIG TYPE: Complex.</p>	<p>Shows the DIRECT REPORTS checkbox.</p> <p>References the Get Multi-User Search Checkbox Restriction.</p>	“Displaying the Checkbox with More Search Options Results” on page 43
MutliUserSearchOption	<p>Used to configure the fields displayed in the SEARCH WITH MORE OPTIONS grid when MORE SEARCH OPTIONS is selected on the USER DETAIL window.</p> <p>The fields are from the Profile table</p> <p>CONFIG TYPE: Complex.</p>		“Specifying Fields for More Search Options” on page 42.
MutliUserSearchResult Fields	<p>Used to configure the fields for MORE SEARCH OPTIONS results on the USER DETAIL window for the multi-user search.</p> <p>The fields are from the Profile table.</p> <p>CONFIG TYPE: Text.</p>		“Displaying the Results for More Search Options” on page 43.

Table 1: The Default Global Options

Global Option (CONFIG NAME)	Description	Default (CONFIG VALUE)	More Information
ResultsPerPage	Configures the number of rows displayed per page in all the grids of the Access Request Manager. CONFIG TYPE: Text	10	
SingleUserSearchKey	Used to configure the unique field for the SEARCH BY <FIELD> on the USER DETAIL window. The unique field is from the Profile table. CONFIG TYPE: Complex.		“Specifying the Unique Search by Field” on page 42.
SingleUserSearchResult Fields	Used to configure the fields displayed for the results of SEARCH BY <FIELD> on the USER DETAIL window. The fields are from the Profile table. CONFIG TYPE: Complex.		“Displaying the Result for Search by Field” on page 43.
UserAccessFields	Used to configure the fields for the USER ACCESS popup that appears on the VERIFY window. The fields are from the Profile table. CONFIG TYPE: Complex.		“Verifying Access Levels” on page 60

Table 1: The Default Global Options

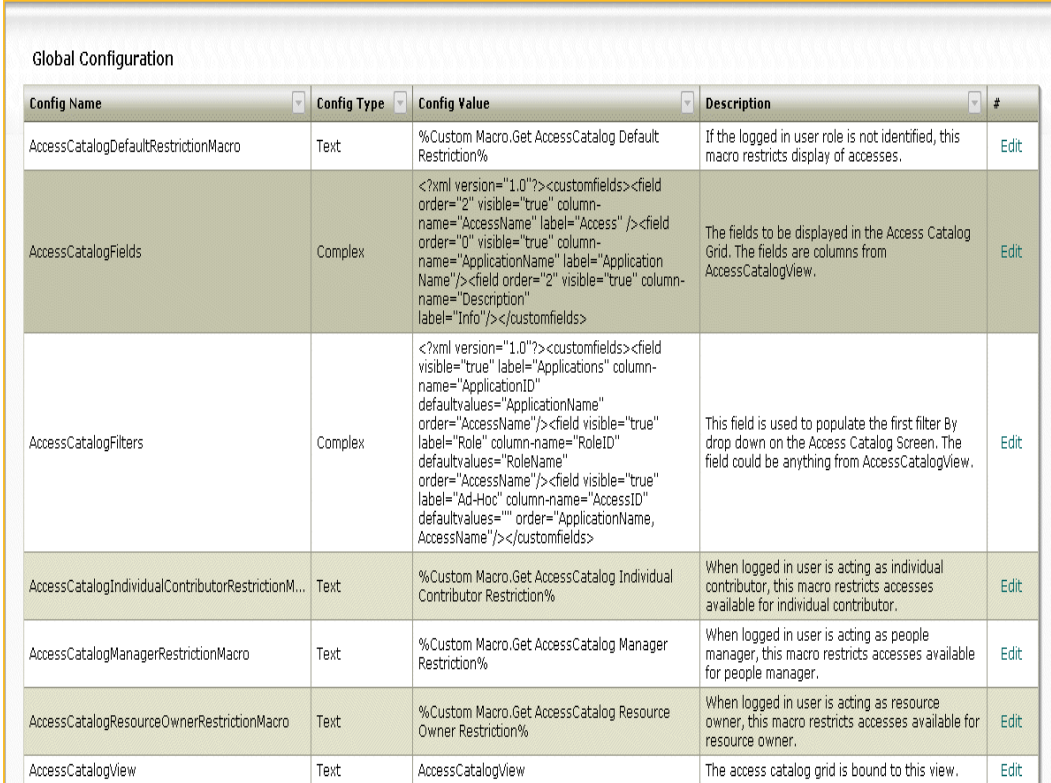
Global Option (CONFIG NAME)	Description	Default (CONFIG VALUE)	More Information
UserSearchDefault RestrictionMacro	<p>Calls the macro that defines the selection restrictions on the USER DETAIL window for a user logging in with an enterprise-specific function.</p> <p>Accepts a custom macro name.</p> <p>CONFIG TYPE: Text.</p>	Get Default Restriction custom macro.	<p>“Constraining the Search Options for Requesters” on page 44</p> <p>For more information about the custom macro the global option references, see “Custom Macros to Implement Default Search Restrictions” on page 45.</p>
UserSearchIndividual ContributorRestriction Macro	<p>Calls the macro that defines the selection restrictions on the USER DETAIL window for a user logging in as an Individual Contributor.</p> <p>Accepts a custom macro name.</p> <p>CONFIG TYPE: Text.</p>	Get Individual Contributor custom macro.	<p>“Constraining the Search Options for Requesters” on page 44</p> <p>For more information about the custom macro the global option references, see “Custom Macros to Implement Default Search Restrictions” on page 45.</p>
UserSearchManager RestrictionMacro	<p>Calls the macro that defines the selection restrictions on the USER DETAIL window for a user logging in as a Business Manager.</p> <p>Accepts a custom macro name.</p> <p>CONFIG TYPE: Text.</p>	Get Manager Restriction	<p>“Constraining the Search Options for Requesters” on page 44</p> <p>For more information about the custom macro the global option references, see “Custom Macros to Implement Default Search Restrictions” on page 45.</p>
UserSearchOptions	<p>Used to configure the display of the search options on the USER DETAIL window.</p> <p>CONFIG TYPE: Complex.</p>	Search by Employee ID More Search Options Add New	<p>“Displaying Radio Buttons for Searching or Adding New Recipients” on page 41</p>

Table 1: The Default Global Options

Global Option (CONFIG NAME)	Description	Default (CONFIG VALUE)	More Information
UserSearchResourceOwnerRestrictionMacro	<p>Calls the macro that defines the selection restrictions on the USER DETAIL window for a user logging in as a Resource Owner.</p> <p>Accepts a custom macro name.</p> <p>CONFIG TYPE: Text.</p>	Get Resource Owner Restriction	<p>“Constraining the Search Options for Requesters” on page 44</p> <p>For more information about the custom macro the global option references, see “Custom Macros to Implement Default Search Restrictions” on page 45.</p>

Editing Global Options

To navigate to the Global Configuration Manager, click **CONFIGURATION** and select **GLOBAL CONFIGURATION MANAGER** from the submenu.

Figure 7: The Global Configuration Manager


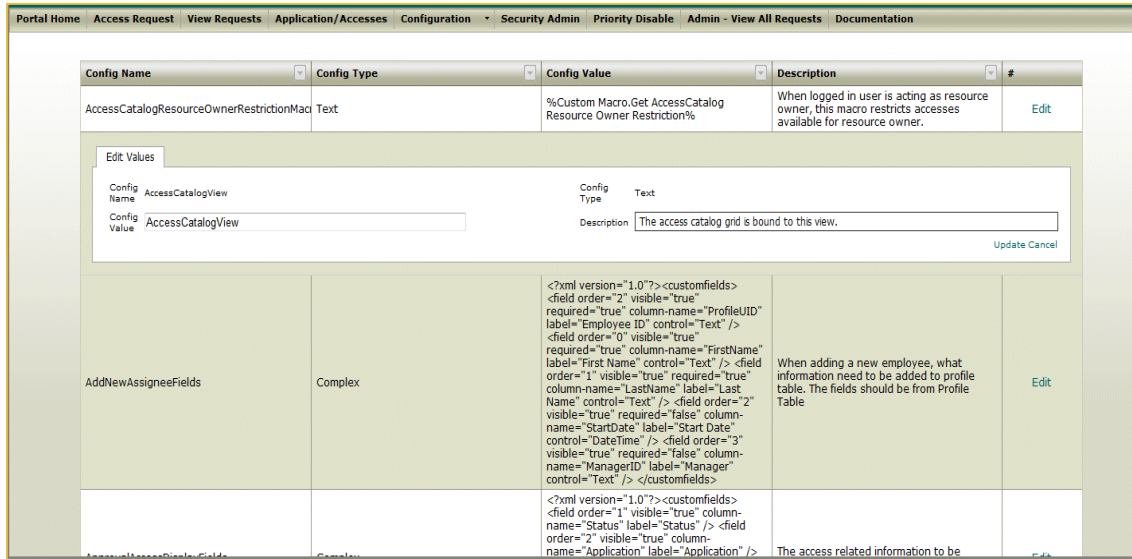
Config Name	Config Type	Config Value	Description	#
AccessCatalogDefaultRestrictionMacro	Text	%Custom Macro.Get AccessCatalog Default Restriction%	If the logged in user role is not identified, this macro restricts display of accesses.	Edit
AccessCatalogFields	Complex	<?xml version="1.0"?><customfields><field order="2" visible="true" column-name="AccessName" label="Access" /><field order="0" visible="true" column-name="ApplicationName" label="Application Name"/><field order="2" visible="true" column-name="Description" label="Info"/></customfields>	The fields to be displayed in the Access Catalog Grid. The fields are columns from AccessCatalogView.	Edit
AccessCatalogFilters	Complex	<?xml version="1.0"?><customfields><field visible="true" label="Applications" column-name="ApplicationID" defaultvalues="ApplicationName" order="AccessName"/><field visible="true" label="Role" column-name="RoleID" defaultvalues="RoleName" order="AccessName"/><field visible="true" label="Ad-Hoc" column-name="AccessID" defaultvalues="" order="ApplicationName, AccessName"/></customfields>	This field is used to populate the first filter By drop down on the Access Catalog Screen. The field could be anything from AccessCatalogView.	Edit
AccessCatalogIndividualContributorRestrictionM...	Text	%Custom Macro.Get AccessCatalog Individual Contributor Restriction%	When logged in user is acting as individual contributor, this macro restricts accesses available for individual contributor.	Edit
AccessCatalogManagerRestrictionMacro	Text	%Custom Macro.Get AccessCatalog Manager Restriction%	When logged in user is acting as people manager, this macro restricts accesses available for people manager.	Edit
AccessCatalogResourceOwnerRestrictionMacro	Text	%Custom Macro.Get AccessCatalog Resource Owner Restriction%	When logged in user is acting as resource owner, this macro restricts accesses available for resource owner.	Edit
AccessCatalogView	Text	AccessCatalogView	The access catalog grid is bound to this view.	Edit

The **GLOBAL CONFIGURATION MANAGER** appears as shown in [Figure 7](#), and shows the default global options.

Editing Global Options with Config Type as Text

To edit a global option with **CONFIG TYPE** as **TEXT**, select **EDIT** for that global option. The **EDIT VALUES** window appears, as shown in [Figure 8](#).

Figure 8: Global Options with Config Type as Text

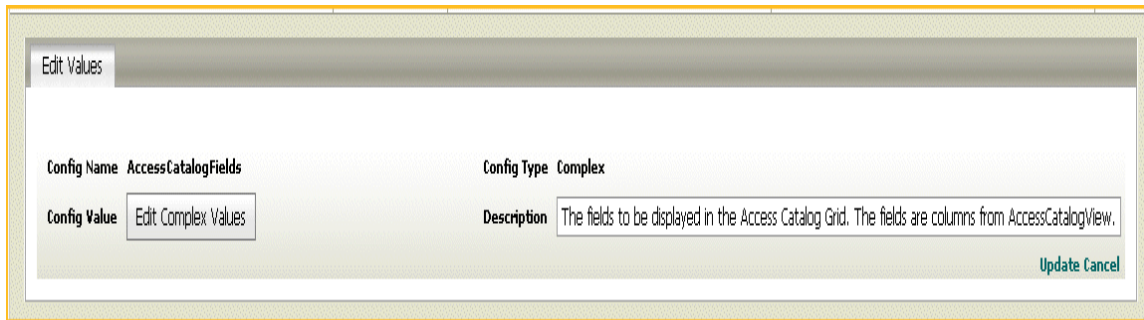


Edit the **CONFIG VALUE** and **DESCRIPTION**. Click **UPDATE** when done.

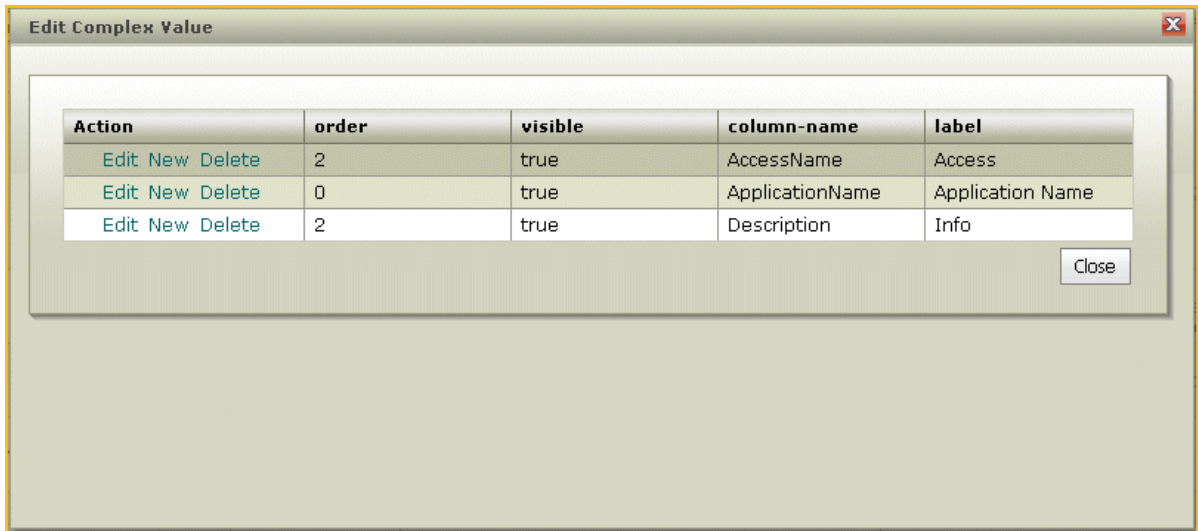
Editing Global Options with Config Type as Complex

To edit a global option with **CONFIG TYPE** as **COMPLEX**, select **EDIT**. For example, select **EDIT** for the **ACCESSCATALOGFIELDS** global option. The **EDIT VALUES** window appears, as shown in [Figure 9](#).

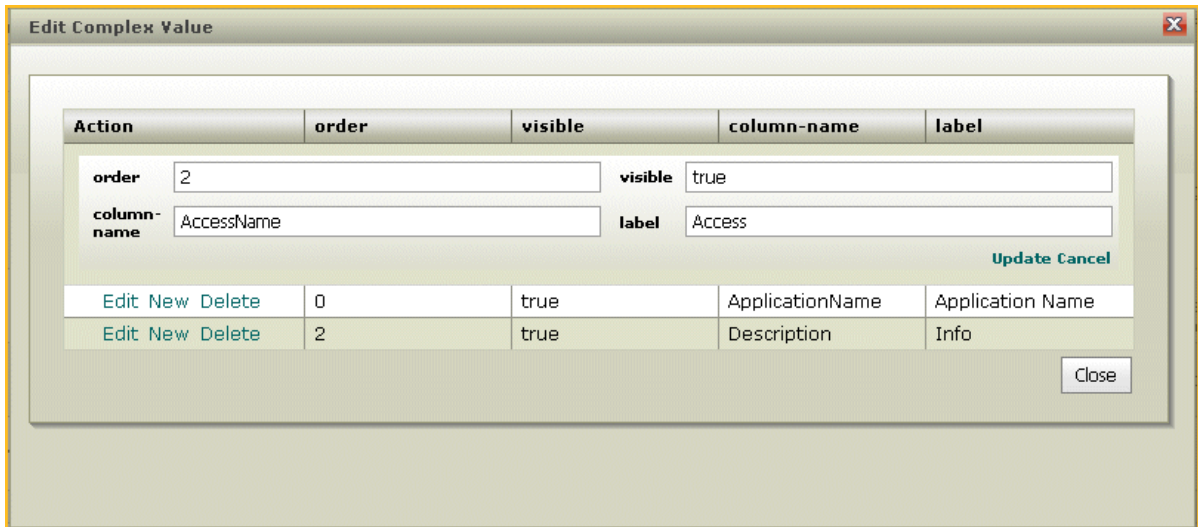
Figure 9: Global Options with Config Type as Complex



Select **EDIT COMPLEX VALUES**. An **EDIT COMPLEX VALUE** editor appears as shown in [Figure 10](#). The editor allows you to **EDIT** values for one or more of the columns, **DELETE** an entire row, or add a **NEW** row to the global option.

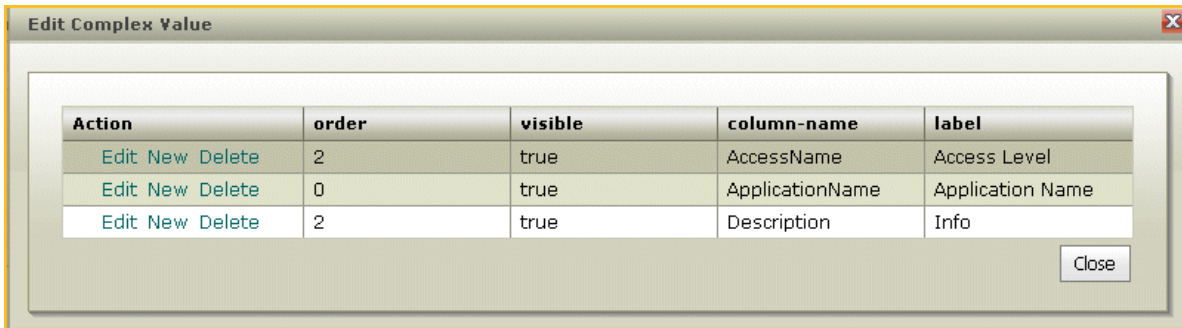
Figure 10: Edit Complex Value Editor

Select **EDIT** to make changes to one or more of the columns. The window in [Figure 11](#) appears allowing you to make changes.

Figure 11: Editing Values for AccessCatalogFields

Change the **LABEL** to Access Level and select **UPDATE**. The window now displays the updated **LABEL** column with Access Level, as shown in [Figure 12](#).

Figure 12: Updated Label for AccessCatalogFields



Action	order	visible	column-name	label
Edit New Delete	2	true	AccessName	Access Level
Edit New Delete	0	true	ApplicationName	Application Name
Edit New Delete	2	true	Description	Info

The **EDIT COMPLEX VALUE** editor displays columns such as **ORDER**, **VISIBLE**, **COLUMN-NAME**, and **LABEL** for the **ACCESSCATALOGFIELDS** global option. Similarly, the editor may display one or more of the following columns for global options with **CONFIG TYPE** as **COMPLEX** mentioned in Table 1 :

- **Order:** Accepts an integer. The fields are displayed in the order specified.
However, for the **ACCESSCATALOGFILTERS** global option, the order attribute accepts a field. The results are sorted by the field specified. For more information, refer to [“Configuring the Primary and Secondary Drop-Down Lists” on page 47](#).
- **Visible:** Accepts a boolean value of true or false. True shows a field and false hides it.
- **Column-name:** Accepts a string. Depending on the context, it identifies a field from a table or identifies an action.
- **Label/Alias:** Accepts a string. Enter a user-friendly alias for a field. This alias appears as the field name on the user windows.
- **Control:** Accepts a string. The data types supported are text, boolean, list and date time. Text displays a textbox, boolean displays a checkbox, list displays a drop-down list, date time displays date time control.
- **Clause:** Accepts a custom macro name.
- **Defaultvalues:** Accepts a string. Specify the information you want to appear as default. For example, if the control data type is a list, the user is shown a drop-down list with default values. The values you specify populate the drop-down list.
- **Required:** Accepts a boolean value of true or false. If it is true, the field requires an input from the user; if it is false, no input is required.
- **Require-comment:** Accepts a boolean value of true or false. If true, the user is required to enter a comment when some action is performed.
- **ImageURL:** Accepts a path for an image.

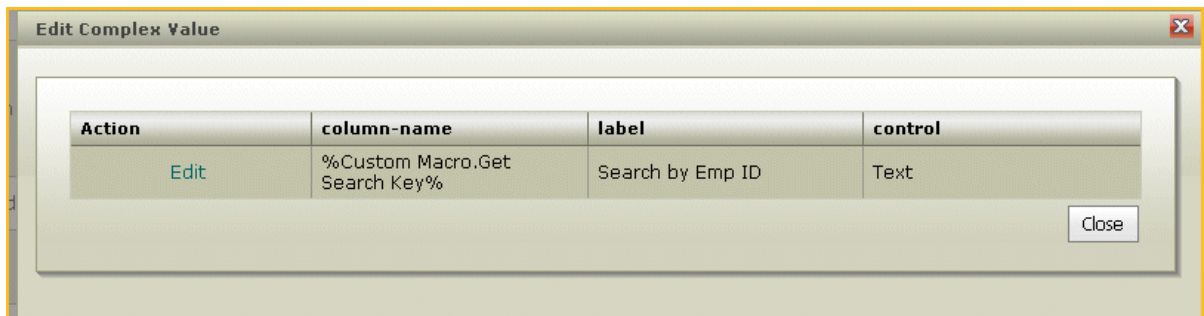
Select **CLOSE** to exit from the editor. Modify the text in the **DESCRIPTION** field, and select **UPDATE** on the **EDIT VALUE** window to save the changes.

Specifying Custom Macros in the Edit Complex Value Editor

Typically, the columns in the **EDIT COMPLEX VALUE** editor described in the section [“Editing Global Options with Config Type as Complex”](#) accept values of a certain type. The columns are also enabled to accept custom macros. For example, the **COLUMN-NAME** column for the **SINGLEUSERSEARCHKEY** global option contains a field name from the Profile table, as shown in [Figure 13](#).

Figure 13: SingleUserSearchKey without a Custom Macro

You can edit the **COLUMN-NAME** for the **SINGLEUSERSEARCHKEY** global option to reference a custom macro, as shown in [Figure 14](#),

Figure 14: SingleUserSearchKey with the Custom Macro

The following columns in the **EDIT COMPLEX VALUE** editor are enabled to accept custom macros and support a return value from the custom macro of the type described for each:

- **Order** - Integer
- **Visible** - Boolean (True or False)
- **Column-name** - String
- **Label** - String
- **Control** - String for data types text, boolean, list and date time.
- **Required** - Boolean (True or False)
- **Require-comment** - Boolean (True or False)
- **Defaultvalues** - String (For control = list, the string should be with comma-separated values).

The custom macros enable you to make the fields configurable and conditional.

Using the Pick List Admin

You can create and manage picklists for the Access Request Manager through the **PICK LIST ADMIN**. A picklist enables you to create a list of pre-defined values from which you can select only one. For example, if you have a drop-down list for Category, you can specify a list of pre-defined values such as Sales, Finance, and Engineering.

This section lists the default picklist types available to you, and describes the general procedure to add a list of values to them.

Default Picklist Types and Values

Table 2: The Default Picklist Types

Default Picklist Types	Picklist Values Supported	Where is the PickList Value Used	Description
ApprovalType	Manager and Secondary	System Use	If the Business Manager approves a request, then the approval type is Manager. If a second-level approver approves the request, the approval type is secondary.
Category	Create enterprise-specific categories for applications. For example, Sales.	Populates the drop-down list for CATEGORY on the APPLICATION/ACCESS MANAGER .	Customize the categories that appear in the drop-down list by modifying this picklist type. The drop-down list enables you to select a category for the application you are adding. For more information about how to select a category to add applications, refer to “Adding Applications” on page 48 .
Severity	Not Applicable	Not Applicable	Not Applicable
Status	<p>Pending - the request is submitted and awaiting approval.</p> <p>Approved - the request is approved.</p> <p>Denied - the request is denied.</p> <p>On Hold - the request is on hold if there are multiple levels of approvals.</p> <p>Processing - the request is in processing until AccountCourier or manual action is taken on the request.</p> <p>Complete - the request is complete if AccountCourier or manual action is taken on the request.</p>	Displayed on the VIEW REQUEST and ADMIN - VIEW ALL REQUESTS windows.	Defines the different states of a request.

Adding a PickList Value

To add a picklist value for a default picklist type, follow these steps:

1. Click **CONFIGURATION** and select **PICK LIST CONFIGURATION** from the drop-down list. The **PICK LIST ADMIN** appears, as shown in [Figure 15](#).

Figure 15: Pick List Admin

PickList Value	PickList Type	Edit	Delete
Accept	Action		
Deny	Action		
Disable	Action		
Ignore	Action		
Investigate	Action		
Remove	Action		
Review	Action		
ServiceAccount	Action		
UserAccount	Action		
Manager	ApprovalType		
Secondary	ApprovalType		
Converge	Category		
Domain Control	Category		
Engineering	Category		

At the bottom of the table, there is a button labeled "Add PickList Item" and a "Refresh" button.

2. Select **ADD PICKLIST ITEM**, as shown in [Figure 16](#).

Figure 16: Add PickList Value and Type

Pick List Admin

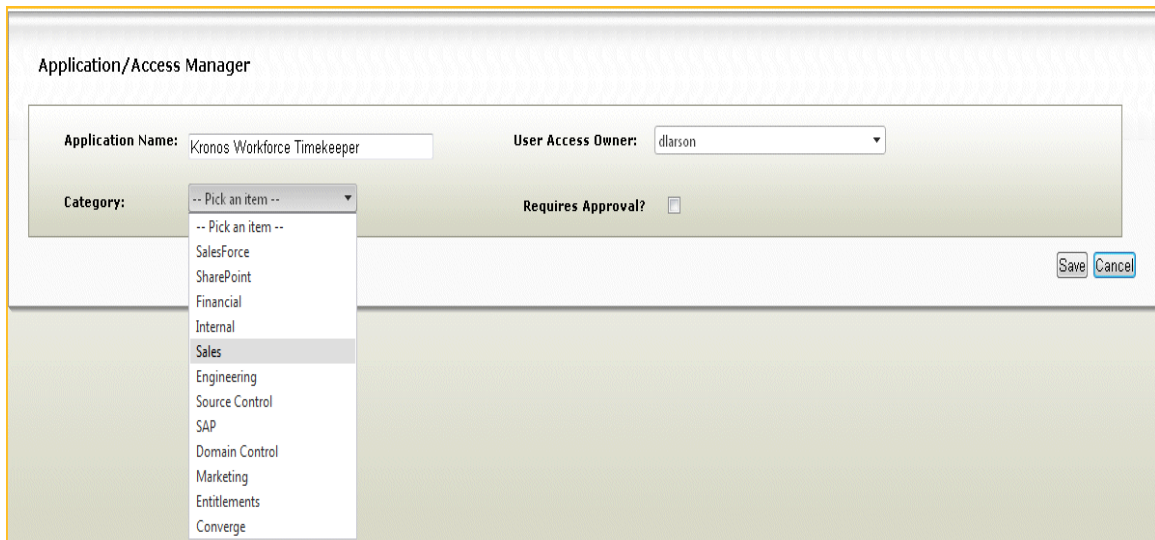
PickList Value	PickList Type	Edit	Delete
PickList Value: <input type="text" value="Sales"/>	PickList Type: <input type="text" value="Category"/>	<input type="button" value="Insert"/>	<input type="button" value="Cancel"/>

Configure the following fields:

PICKLIST VALUE: Add a customized value for the picklist type. For example, add Sales.

PICKLIST TYPE: Add a picklist type from the defaults available, for example "Category." Refer to Table 2 .

The picklist type, Sales, populates the **CATEGORY** drop-down list in the **APPLICATION/ACCESS MANAGER**, as shown in [Figure 17](#).

Figure 17: Example of the PickList Item in the Application/Access Manager

The screenshot shows the 'Application/Access Manager' interface. It features a form with the following fields:

- Application Name:** Kronos Workforce Timekeeper
- User Access Owner:** dlarrison
- Category:** A dropdown menu is open, showing a list of categories: -- Pick an item --, SalesForce, SharePoint, Financial, Internal, Sales (highlighted), Engineering, Source Control, SAP, Domain Control, Marketing, Entitlements, and Converge.
- Requires Approval?:**

At the bottom right of the form, there are 'Save' and 'Cancel' buttons.

3. Select **INSERT** to add it to the **PICK LIST ADMIN**.

Click the Edit icon  to edit, or the Delete icon  to delete a picklist value.

Chapter 4: Configuring the Access Request Workflow

This chapter describes how to use the Administration Interface to configure the request workflow, and includes the following sections:

- [“Selecting Recipients” on page 40](#) - Describes how to configure the **USER DETAIL** window to enable a requester to select recipients.
- [“Selecting Access Levels” on page 47](#) - Describes how to configure the **ACCESS CATALOG** window for adding access levels. You must first add applications before you add any access levels for it.
- [“Adding Roles” on page 55](#) - Describes how to add roles and map access levels to them for the **ACCESS CATALOG** window.
- [“Verifying Access Levels” on page 60](#) - Describes how to configure the **VERIFY** window for the requester to manage the access levels.

Before you configure the **USER DETAIL**, **ACCESS CATALOG** and **VERIFY** windows, review the section [“Using the Global Configuration Manager” on page 21](#) that describes the global options used in this chapter and how to edit them.

Selecting Recipients

This section describes how to configure the **USER DETAIL** window to enable a requester to search for recipients consistent with the policies specific to your enterprise. The requesters can select themselves as the recipients or select others, depending on the enterprise policy. You can configure the following on the **USER DETAIL** window:

- The category of the recipient the requester can select, such as **EMPLOYEE** or **CONTRACTOR**.
- The radio buttons that enable the requester to search for recipients or add a new recipient.
- The unique search field by which a requester can look up a recipient. You can configure a user-friendly label for the unique field. You can also configure which fields to show when displaying information about the recipient who matches the search criterion.
- The fields for a requester to do an advanced search based on broader criteria to select multiple recipients. You can configure user-friendly labels for the field names. You can also configure which fields to show when displaying information about the recipients who match the search criteria.
- The required and optional fields that the requester must enter when they enter new recipient information.

This section includes the following:

- [“Specifying Categories for the Providing Access For Drop-Down List” on page 40](#)
- [“Setting Up the Search to Look for Recipients” on page 41](#)
- [“Displaying the Search Results” on page 42](#)
- [“Constraining the Search Options for Requesters” on page 44](#)

Specifying Categories for the Providing Access For Drop-Down List

The **PROVIDING ACCESS FOR** drop-down list on the **USER DETAIL** window displays the default **EMPLOYEE**, **CONTRACTOR**, and **MYSELF** categories to search for recipients. These categories are populated from the UserType table.

To customize the list, add a new category in to the UserType table, or change the default **EMPLOYEE** and **CONTRACTOR** names. To add a new category:

1. Add a new record into the UserType table with the following fields, for example:
 - UserTypeID = System-generated number
 - Name = Part-time Employee
 - Label = Part-Time
 - Description = A person who works for 20 hours or less.
2. Map the UserType table to the Profile Table, which contains all the profile information. For example, if you have an entry in the Profile table for a part-time employee, update the UserType field for that record:
 - ProfileUID = EMP123

FirstName = Jack

LastName = Smith

Job Title = Part-time Consultant

UserType = Enter the system-generated number

Note: To map the two tables, the number in the UserType field must match the UserTypeID field of the Usertype table.

The new category, Part-Time, appears as a new category in the **PROVIDING ACCESS FOR** drop-down list. If a requester selects this category, Jack Smith will appear in the result displayed.

Displaying Radio Buttons for Searching or Adding New Recipients

Search options on the **USER DETAIL** window enable a requester to look up recipients or add a new recipient if none is found using the search. Use the **USERSEARCHOPTIONS** global option to configure the search options. This global option is entered as an XML string. Table 3 shows the default values for **USERSEARCHOPTIONS**.

Table 3: UserSearchOptions Default Values

Visible	Column-name	Label	DefaultValues
True	SingleUserSearch	None	True
True	MoreSearch	More Search Options	False
True	AddNew	Add New	False

The search options appear as radio buttons. The SingleUserSearch column-name displays the label **SEARCH BY EMPLOYEE ID** in the **SingleUserSearchKey** global option, as described in the section [“Specifying the Unique Search by Field” on page 42](#). The **SEARCH BY EMPLOYEE ID** radio button is selected by default.

Setting Up the Search to Look for Recipients

You can configure the search options so that a requester can search:

- Using a unique field
- Using the advanced search to look up multiple recipients.

Specifying the Unique Search by Field

A requester can search on a unique field entry for a single recipient. You can configure the **SINGLEUSERSEARCHKEY** global option to specify a field from the Profile table that is unique. If the field you configure contains duplicate values, the search will return the first record that matches the value entered for the single user search option. This global option is entered as an XML string. Table 4 shows the default values for **SINGLEUSERSEARCHKEY**.

Table 4: SingleUserSearchKey Default Values

Column-name	Label	Control
ProfileUID	Search by Employee ID	Text

The field you configure appears on the **USER DETAIL** window. The requester can search for a recipient by using the unique user-identifier field.

Specifying Fields for More Search Options

Using the **MORE SEARCH OPTIONS** selection, a requester can search for multiple recipients with a broader set of search criteria. You can configure the **MULTIUSERSEARCHOPTION** to specify the fields from the Profile table that provides the search options. You enter the **MULTIUSERSEARCHOPTION** as an XML string. Table 5 shows the default values for **MULTIUSERSEARCHOPTION**.

Table 5: MultiUserSearchOption Default Values

Order	Visible	Column-name	Label	Control	Defaultvalues
0	True	ProfileUID	Employee ID	Text	None
1	True	FirstName	First Name	Text	None
2	True	LastName	Last Name	Text	None
3	True	StartDate	Start Date	DateTime	None
4	True	Location	Location	List	Enter a comma-separated list of default values for the drop-down list.

Displaying the Search Results

You can customize how a search result is shown on the **USER DETAIL** window.

Displaying the Result for Search by Field

When a requester searches for a recipient using the **SEARCH BY <FIELD>**, the result appears in the **SEARCH RESULTS**. You can configure **SINGLEUSERSEARCHRESULTFIELDS** to specify the fields to display from the Profile table for recipient information. This global option is entered as an XML string. Table 6 shows the default values for **SINGLEUSERSEARCHRESULTFIELDS**.

Table 6: SingleUserSearchResultFields Default Values

Column-name	Order	Label	Visible
FirstName	0	First Name	True
LastName	1	Last Name	True
ProfileUID	2	Employee ID	True
RoleID	3	Role ID	True
DeleteHold	4	Hold Delete	True
StartDate	5	Start Date	True
ManagerID	6	Manager	True
Location	7	Office Location	True

Displaying the Results for More Search Options

When a requester searches for a recipient using the **MORE SEARCH OPTIONS**, the results appear in the **SEARCH RESULTS** popup. You can configure **MULTIUSERSEARCHRESULTFIELDS** to specify the fields to display from the Profile table for recipient information.

Displaying the Checkbox with More Search Options Results

By default the **DIRECT REPORTS** checkbox appears unchecked when a requester uses the **MORE SEARCH OPTIONS** to look up recipients. To change the label and restrict whether or not to display the checkbox, use the **MULTIUSERSEARCHRESTRICTION**. This global option is entered as an XML string, which also references the macro, **GET MULTI-USER SEARCH CHECKBOX RESTRICTION**. For more information on the macro, refer to [“Custom Macros to Implement Default Search Restrictions” on page 45](#). Table 7 shows the default values for **MULTIUSERSEARCHRESTRICTION**.

Table 7: MultiUserSearchRestriction Default Values

Visible	Label	Clause	DefaultValues
True	Direct Reports	%Custom Macro.Get Multi-User Search Checkbox Restriction%	False

Configuring fields to Add a New Recipient

To enable a requester to add a new recipient, customize the list of fields that appear on the **USER DETAIL** window for the **ADD NEW** option. The information entered by the requester is stored in the Profile table. To configure the XML string, specify the fields from the Profile table for the **ADDNEWASSIGNEEFIELDS** global option.

Table 8 shows the default values for **ADDNEWASSIGNEEFIELDS**. Modify the XML string to change an

Table 8: AddNewAssigneeFields Default Values

Column-name	Order	Required	Visible	Label	Control	Default values
ProfileUID	0	True	True	Employee ID	Text	None
FirstName	1	True	True	First Name	Text	None
LastName	2	True	True	Last name	Text	None
StartDate	3	True	False	Start Date	DateTime	None
Location	5	True	False	Location	List	Enter a list of default values for the drop-down list.

XML attribute or value.

Constraining the Search Options for Requesters

You can restrict which recipients the requesters can select depending on the function of the requesters logging in to the Access Request Manager. For example, if Business Managers log in to the Access Request Manager, by default they can select only their direct reports.

The following global options are used to determine the restrictions on the selection of recipients:

- **USERSEARCHDEFAULTRESTRICTIONMACRO** - References the Get Default Restriction custom macro that implements restrictions on a requester logging in with an enterprise-specific function, such as a Business Manager.
- **USERSEARCHINDIVIDUALCONTRIBUTORRESTRICTIONMACRO** - References the Get Individual Contributor custom macro that implements restrictions on a requester logging in as an Individual Contributor.
- **USERSEARCHMANAGERRESTRICTIONMACRO** - References the Get Manager Restriction custom macro that implements restrictions on a requester logging in as a Business Manager.
- **USERSEARCHRESOURCEOWNERRESTRICTIONMACRO** - References the Get Resource Owner Restriction custom macro that implements restrictions on a requester logging in as a Resource Owner.

Custom Macros to Implement Default Search Restrictions

The Access Request Manager provides custom macros described in Table 9 to implement default restrictions on recipients displayed on the **USER DETAIL** window. Search restrictions determine which recipients the requesters can see, based on their functions, while making a request.

Table 9: Custom Macros that Implement Search Restrictions

Custom Macro	Default Restriction
Get Default Restriction	If requesters with enterprise-specific functions make requests, the macro allows them to see all users by default. For example, if a new Project Manager function is added, then a requester with this function sees all users.
Get Individual Contributor Restriction	<p>If Individual Contributors make a request, the macro by default allows them to see only themselves.</p> <p>Customize the restriction to search for all users instead of only the Individual Contributor. Additionally, implement other restrictions, such as:</p> <ul style="list-style-type: none"> • Allow Individual Contributors to see all users in their department. • Allow Individual Contributors to see all users in their department, and at their location.
Get Manager Restriction	<p>If Business Managers search for recipients to make a request, the macro by default allows them to see only their direct reports.</p> <p>This macro contains a value that enables the search to be changed from direct reports only to all employees. Implement other restrictions, such as:</p> <ul style="list-style-type: none"> • Allow Business Managers to see all candidate recipients in their department. • Allow Business Managers to see all candidate recipients in their department and at their location.
Get Multi-User Search Checkbox Restriction	<p>The macro searches only for direct reports by default when the requester selects the checkbox.</p> <p>Implement a new restriction so that when requesters, such as Business Managers, search for multiple users, they see direct reports from their location.</p>
Get Resource Owner Restriction	<p>If Resource Owners search for recipients to make a request, the macro by default allows them to see all users.</p> <p>Implement a new restriction such that the Resource Owner sees only those recipients who are in a particular division or location, or set of locations.</p>

Custom Macros to Retrieve User Information

The Access Request Manager provides the custom macros described in Table 10 to retrieve information about a user who logs in to make a request, approve a request or perform administrative tasks.

Table 10: Custom Macros to Retrieve User Information

Custom Macro	Information Retrieved
Get LoggedInUser Name	The macro retrieves the user name of the logged in user: the requester, the approver, or the administrator.
Get LoggedInUser Role	<p>The macro retrieves the function of the logged in user. By default, the Access Request Manager supports users with the following functions:</p> <ul style="list-style-type: none"> • Individual Contributor, also known as a Business User • Business Manager • Resource Owner <p>Add new enterprise-specific functions, such as Project Manager or Contractor Manager to expand the list of functions.</p>

Selecting Access Levels

This section describes how to configure the **ACCESS CATALOG** window for requesters to add access levels consistent with the policies and processes specific to your enterprise. You can configure the following items on the **ACCESS CATALOG** window:

- The primary and secondary drop-down lists.
- Applications and access levels the requester can select. You can also configure the fields to show when displaying access levels.
- The popup that appears when a requester selects an access level.
- Roles and the mapped access levels the requester can select.

This section includes the following:

- [“Configuring the Primary and Secondary Drop-Down Lists” on page 47.](#)
- [“Adding Access Levels” on page 50.](#)
- [“Adding Target Attributes” on page 51.](#)
- [“Configuring the Access Level Fields Displayed to the Requester” on page 58.](#)
- [“Constraining the Access Levels Visible to Requesters” on page 58](#)

Configuring the Primary and Secondary Drop-Down Lists

The primary and secondary drop-down lists enable requesters to filter the access levels they can select. You configure the **ACCESSCATALOGFILTERS** global option to customize the contents of the primary and secondary drop-down lists. This global option is entered as an XML string, and it retrieves information from AccessCatalogView.

For example, if you want to add Department to the drop-down lists:

1. Update the AccessCatalogView to have the fields DepartmentID and DepartmentName.
2. Update the XML string in the **ACCESSCATALOGFILTERS**. For example:

```
<field visible="true" label=""Department" column-
name="DepartmentID" defaultvalues="DepartmentName" />
<customfields>
<field visible="true" label="Applications" column-
name="ApplicationID" defaultvalues="ApplicationName" />
<field visible="true" label="Role" column-name="RoleID"
defaultvalues="RoleName" />
<field visible="true" label="Ad-Hoc" column-name="AccessID"
defaultvalues="" />
</customfields>
```

The Department option with a list of all the available departments appear in the drop-down lists.

Table 11 shows the default values for **AccessCatalogFilters**.

Table 11: AccessCatalogFilters Default Values

Column-name	Label	Defaultvalues	Order	Visible
ApplicationID	Applications (Displayed in the primary drop-down list).	ApplicationName (Displays the name of the applications in the secondary drop-down list).	AccessName	True
RoleID	Role (Displayed in the primary drop-down list).	RoleName (Displays the name of the roles in the secondary drop-down list).	AccessName	True
AccessID	Ad-Hoc (Displayed in the primary drop-down list).	No secondary drop-down list is displayed.	Application Name, AccessName	True

Note: The order attribute in the XML string allows you to sort the display of the access level results by the field you specify. For example, selecting **APPLICATION** sorts the results in the **FILTER RESULTS** grid by the name of the access levels.

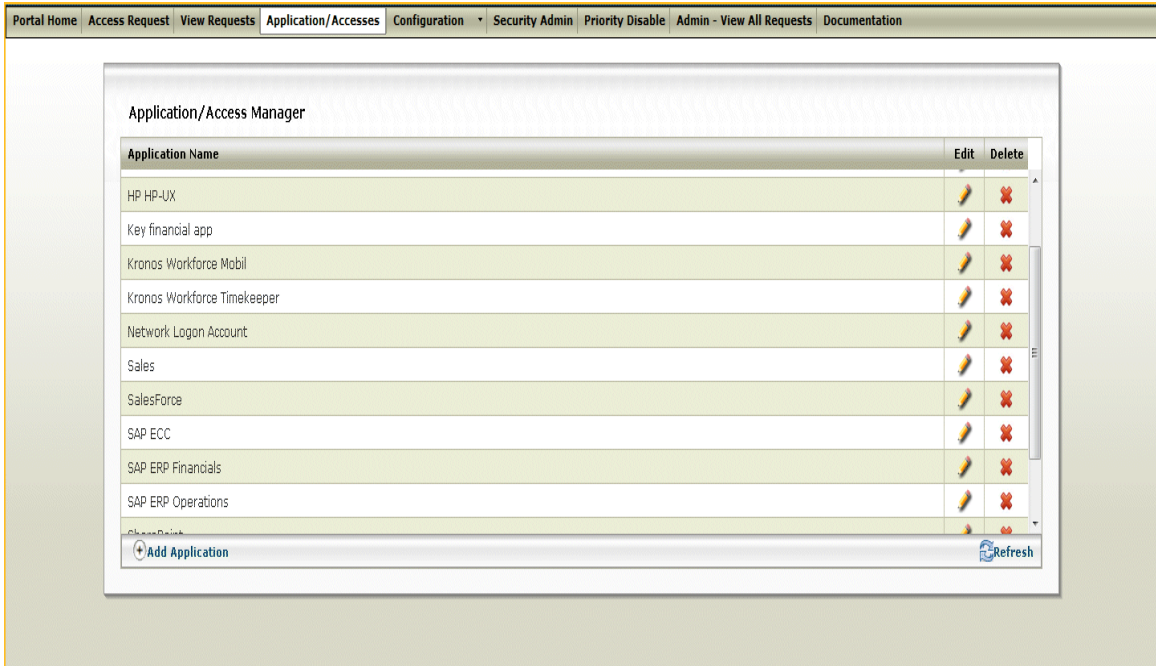
Adding Applications

When a requester selects **APPLICATIONS** from the primary drop-down list, the secondary drop-down list appears with a list of all the applications. The requester then selects one application, such as Microsoft Active Directory, and all the access levels associated with Microsoft Active Directory will appear.

To configure the list of applications and the relevant access levels use the **APPLICATION/ ACCESS MANAGER**. Add applications by following these steps:

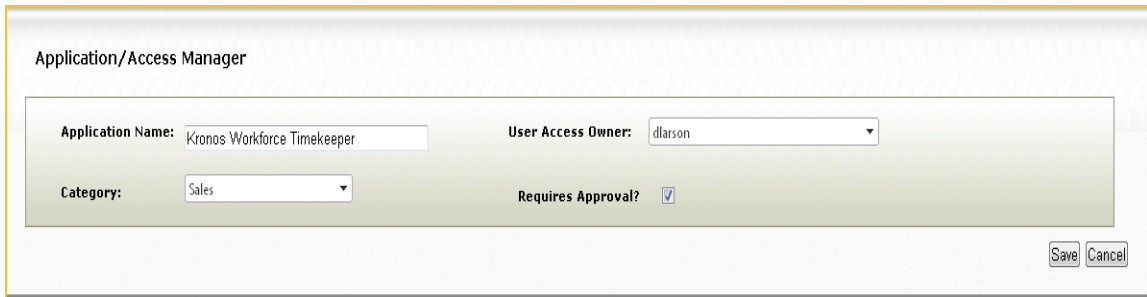
1. Select **APPLICATION/ACCESSES** from the top-level menu. The **APPLICATION/ACCESS MANAGER** appears, as shown in [Figure 18](#).

Figure 18: The Application/Access Manager



2. Click **ADD APPLICATION**. The window to add an application appears, as shown in [Figure 19](#).

Figure 19: Add Application Details



Configure the following fields:

APPLICATION NAME: Enter an application name. The application name added here is shown in the secondary drop-down list, as shown in [Figure 20](#).

USER ACCESS OWNER: Select the name of the Resource Owner. The information for the drop-down list is retrieved from the Profile table.

CATEGORY: Select a category from the drop-down list for the application.

Note: You must populate the drop-down list with customized picklist values. Refer to the section [“Using the Pick List Admin” on page 34](#) for additional information.

REQUIRES APPROVAL?: Check if the application requires approval from a second-level approver. To add an approver, refer to the section [“Adding Second-Level Approvers” on page 62](#).

3. Click **SAVE** to add the application.
4. The grid to add access levels appears. See the section [“Adding Access Levels”](#) for more information.

If you prefer adding access levels later, select **CLOSE** to return to the main **APPLICATION/ACCESS MANAGER**.



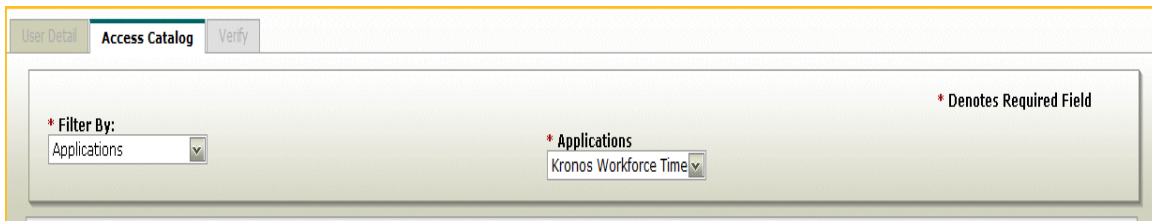
To edit or delete applications, go to the main window of the **APPLICATION/ACCESS MANAGER** by selecting **APPLICATION/ACCESSES** from the top-level menu. Click the Edit icon  to edit, or the Delete icon  to delete an application.

Figure 20: Access Catalog Window with the Secondary Drop-Down List



Adding Access Levels

You can add access levels for an application added earlier through the **APPLICATION/ACCESS MANAGER**. If the application for which you want to add the access level is not available, add it first before proceeding with adding access levels. See [“Adding Applications” on page 48](#) for additional information.

The access levels you add for an application appear in the **FILTER RESULTS** grid on the **ACCESS CATALOG** window.

To add an access level:


1. Select **APPLICATION/ACCESSES** from the top-level menu. The **APPLICATION/ACCESS MANAGER** appears.
2. Click the Edit icon  to edit the application. A window appears with the application details.
If you start with adding a new application and saving it, the window expands to enable you to add access levels.
3. Click **ADD ACCESS**, as shown in [Figure 21](#).

Figure 21: Add Access Levels

Application/Access Manager

Application Name: Kronos Workforce Timekeeper User Access Owner: dlarson

Category: Sales Requires Approval?

Access Levels

Access Name	Description	Severity	Edit	Delete
WFC Exempt	Employee Exempt	Low		

No records to display.

+ Add Access Refresh

Save Close

Configure the following fields in the grid:

ACCESS NAME: Add a name for the access level. This appears in the **ACCESS** column of the **FILTER RESULTS** grid.

DESCRIPTION: Provide a brief description about the access level you entered. This information appears as the mouse-over text for the Info icon on the **ACCESS CATALOG** window.

SEVERITY: Select the severity for the access level.

4. Click **SAVE** to add the access level.

To edit an access level, click the Edit icon .

To delete an access level, click the Delete icon .

The access level you added is shown in the **FILTER RESULTS** grid of the Access Catalog window:

- When a requester selects the associated application from the secondary drop-down list.
- When you assign it to a role, and if the requester selects that role. To assign an access level to a role, refer to [“Adding Roles” on page 55](#).
- When the requester selects **AD-HOC**.

Adding Target Attributes

Once requesters have selected access levels, they can provide additional target attribute information through a popup.

You can decide to show or hide the popup by configuring the fields accordingly. To configure the popup and add target attributes, select an access level through the **APPLICATION/ACCESS MANAGER**. If the access level is not available, add it first before proceeding with adding target attributes.

To configure the popup and add target attributes:


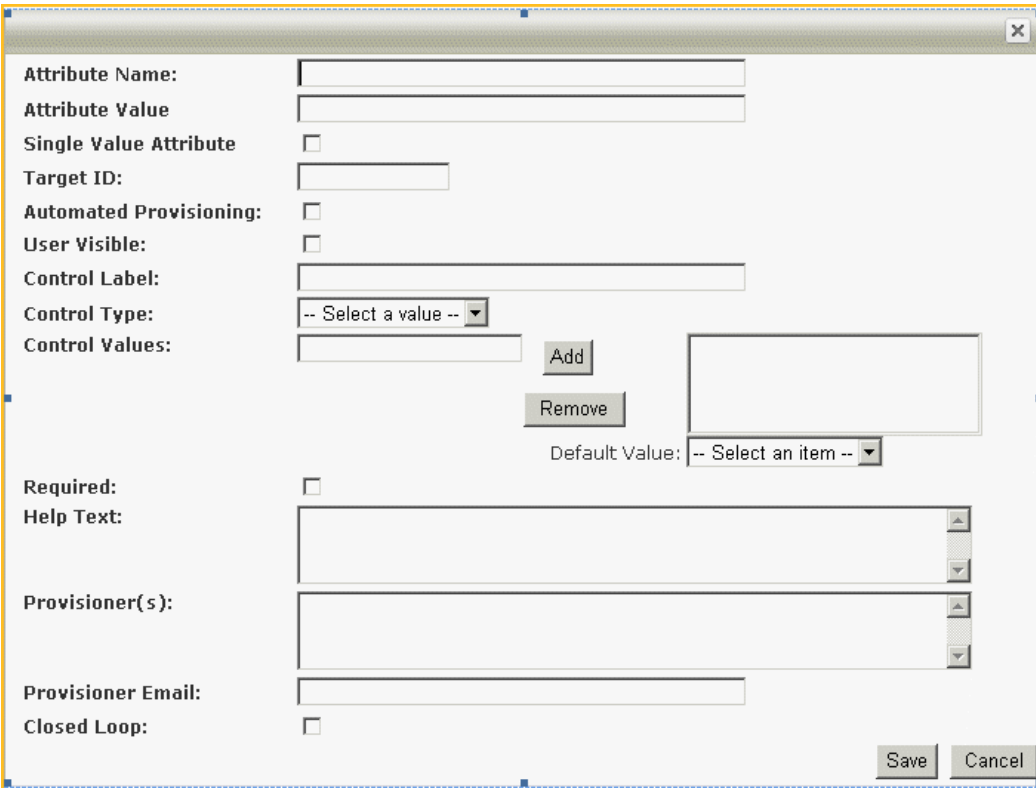
1. Select **APPLICATION/ACCESSES** from the top-level menu. The **APPLICATION/ACCESS MANAGER** appears.
2. Click the Edit icon  to edit the application. A window appears with the application and related access levels.
3. Click **SELECT** in the **ACCESS LEVELS** grid to add a target attribute for a specific access level. The **TARGET ATTRIBUTES** grid appears.
4. Select **ADD ATTRIBUTE** to add a target attribute. A window appears for you to enter the details as shown in [Figure 22](#).

Figure 22: Window to Enter Target Attributes



Configure the following fields:

ATTRIBUTE NAME: Enter a unique name for the attribute. This is a required field.

ATTRIBUTE VALUE: Enter a value for the attribute if you are selecting **TEXTBOX** from the **CONTROLTYPE**. The value you enter appears as the default on the popup displayed to the user. For example, if you enter \$500 and select **TEXTBOX** as the **CONTROL TYPE**, the amount is shown in the textbox.

If you are selecting **CHECKBOX** from the **CONTROL TYPE**, then enter true or false in this field. True will display the checkbox as checked; false will display the checkbox as unchecked.

The **ATTRIBUTE VALUE** field must contain a value if **USER VISIBLE** is unchecked. It is optional if **USER VISIBLE** is checked.

SINGLE VALUE ATTRIBUTE: Check if the **CONTROL TYPE** is a **TEXTBOX** or a **CHECKBOX**; uncheck if the **CONTROL TYPE** is a **DROPDOWNLIST**.

TARGET ID: Enter the details about the target. Refer to the manual *Configuring Workflows with the Access Assurance Suite Administration Manager* for more information about Target IDs.

This is a required field.

AUTOMATED: Check if the access to the target is done automatically through a connector. Uncheck if it is done manually.

USER VISIBLE: Check if you want to show the popup to the requester; uncheck if you want to hide it.

If this field is checked, the requester is able to see the popup and enter additional target attribute information.

If this field is unchecked, no popup is displayed to the requester. In this scenario, the request service automatically obtains the target attribute information from your configuration to process the request.

CONTROL LABEL: Enter the text that will appear as the label on the popup. For example, Amount to Approver is the text that appears as the label in [Figure 23](#).

This is a required field if **USER VISIBLE** is checked. It sets the value for the Custom Control field to true.

Leave the field blank if **USER VISIBLE** is unchecked. It sets the Custom Control field to false.

CONTROL TYPE: Select the control type from the drop-down list. The defaults are **TEXTBOX**, **RADIOBUTTON**, **CHECKBOX**, and **DROPDOWNLIST**.

This is a required field if **USER VISIBLE** is checked.

CONTROL VALUES: Add a list of values to show to the requester if you are selecting either **DROPDOWNLIST** or **RADIOBUTTON** for the **CONTROLTYPE**.

To delete a value, select **REMOVE**.

DEFAULT VALUE: Select a value from the list of **CONTROL VALUES** you added. This is the default that is displayed to the user if the **CONTROLTYPE** is a **DROPDOWNLIST** or a **RADIOBUTTON**.

REQUIRED: Check if requesters are required to provide any configuration information on the popup. The access level is only added when the requester provides the required information.

HELP TEXT: Enter information you want for your reference.

PROVISIONER(S): Enter the name of the person who will do the provisioning if the target is provisioned manually.

PROVISIONER EMAIL: Enter the email of the provisioner to notify about a pending provisioning action.

CLOSED LOOP: Reserved for future use.

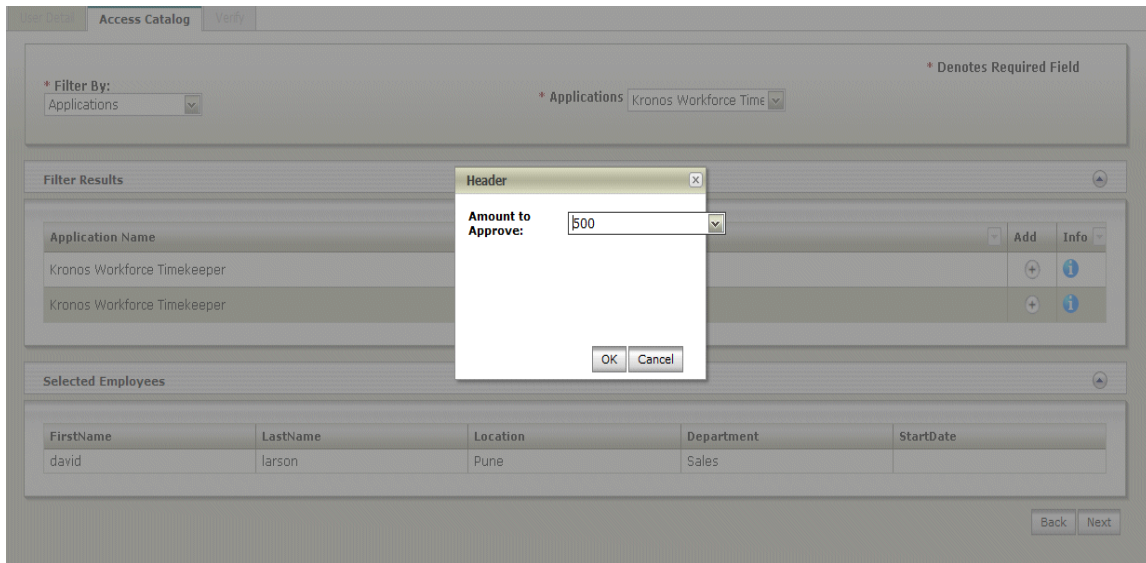
5. Click **SAVE** when done.

To edit an attribute, click the Edit icon  .

To delete an attribute, click the Delete icon  .

The target attribute details you configured appear on the popup on the **ACCESS CATALOG** window. As shown in [Figure 23](#), the requesters are required to select an amount from the drop-down list before they can proceed with their requests.

Figure 23: Access Catalog with the Popup



Adding Roles

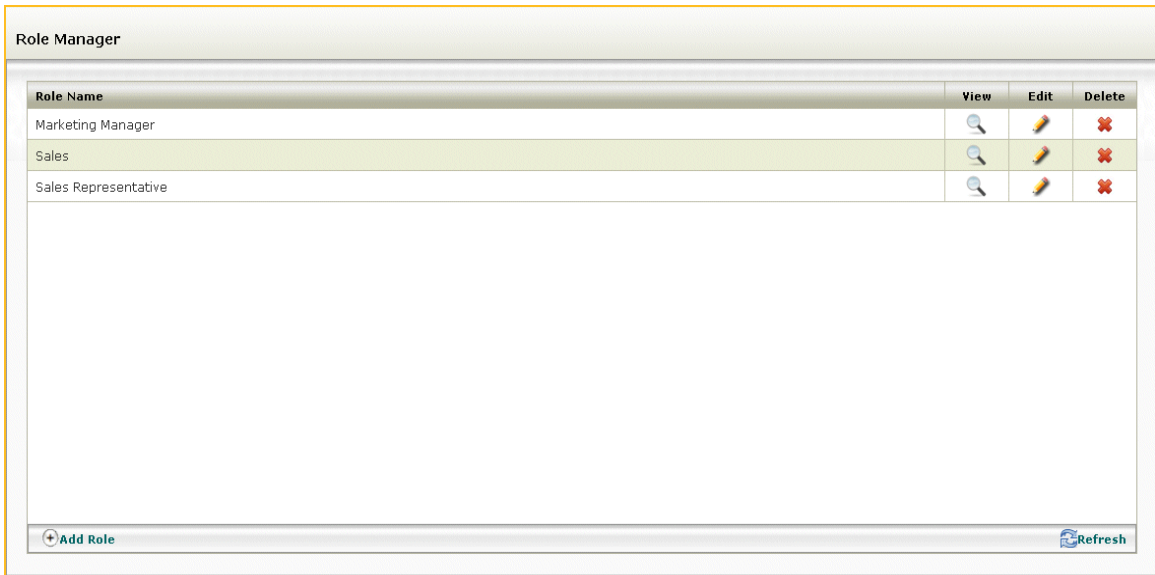
This section describes how to configure the **ACCESS CATALOG** window to display access levels that are mapped to roles. Requesters can then select access levels by roles when provisioning recipients with requests.

A role is defined as a set of access levels. If the requester selects a role, the access levels associated with that role are displayed. The requester can select one or more of the access levels for the recipient.

You can add new roles and map them to existing access levels through the **ROLE MANAGER**. To add a new role, follow these steps:

1. Click **CONFIGURATION** and select **ROLE/ACCESS MAPPING** from the drop-down list. **THE ROLE MANAGER** appears as shown in [Figure 24](#).

Figure 24: Role Manager



The screenshot shows the 'Role Manager' window. It contains a table with three columns: 'Role Name', 'View', 'Edit', and 'Delete'. The table lists three roles: 'Marketing Manager', 'Sales', and 'Sales Representative'. Each role has a magnifying glass icon for 'View', a pencil icon for 'Edit', and a red 'X' icon for 'Delete'. At the bottom left, there is a '+ Add Role' button, and at the bottom right, there is a 'Refresh' button.

Role Name	View	Edit	Delete
Marketing Manager			
Sales			
Sales Representative			

2. Click **ADD ROLE**. The window to add a new role appears, as shown in [Figure 25](#).

Figure 25: Add New Role

3. On **ROLE DETAIL**, enter a name for the role in the **ROLE NAME** field such as Marketing Manager.
4. Select a user from the **USER MINING** drop-down list and click add. After adding the users, click **MINE** if you want to see the access levels the selected users have. The access levels appear in the window. Check **INCLUDE** if you want to add a specific access level to the role you are creating.
5. Click **NEXT STEP** to proceed to the **ACCESS CATALOG** window and select access levels. **ACCESS CATALOG** appears as shown in [Figure 26](#).

Figure 26: Add Access Levels to Roles

Application Name	Access Level	Info	Add
Sales	Sales Archive		
Sales	Sales Contacts		
Sales	Inside Sales Engineer		
Sales	Sales DB Admin		

6. Select an option from the **FILTER BY** drop-down list. A second drop-down list appears grouped by the option you selected. In [Figure 26](#) for example, selecting Application displays a new drop-down list labelled **APPLICATION**. Selecting an application from the second drop-down list displays all the access levels associated with it.


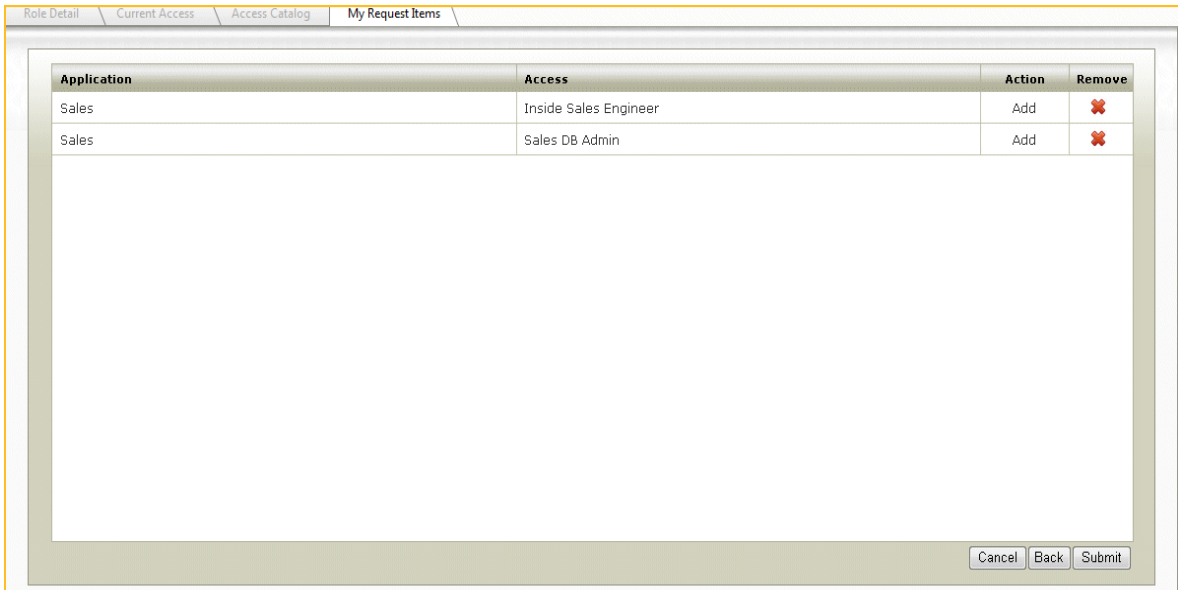

7. Add the access levels using the Add icon  . Click **NEXT STEP. MY REQUEST ITEM** appears, as shown in [Figure 27](#).

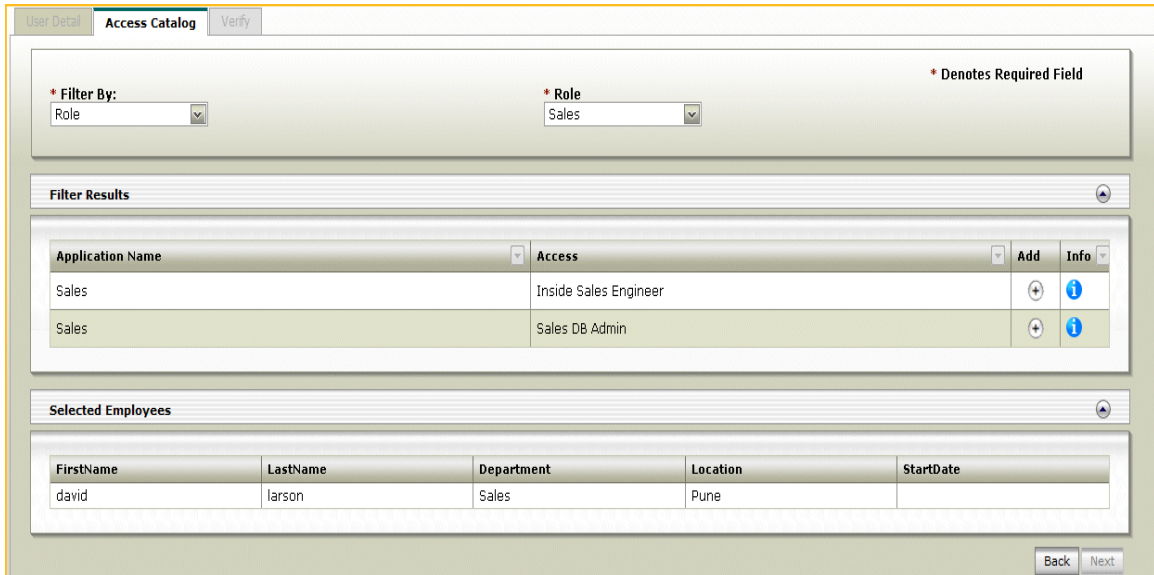
Figure 27: Confirm the Access Levels



8. Delete any access level you want by clicking the Remove icon  . Verify and click **SUBMIT**.

The new role you configured appears on the **ACCESS CATALOG** window of the Access Request Manager, as shown in [Figure 28](#).

Figure 28: Access Catalog Window with Roles



Configuring the Access Level Fields Displayed to the Requester

Requesters can select access levels from the **FIELD RESULTS** grid on the **ACCESS CATALOG** window to add to their request. You can specify which fields to show from the `AccessCatalogView` view by configuring the **ACCESSCATALOGFIELDS** global option.

Table 12 shows the default values for **ACCESSCATALOGFIELDS**.

Table 12: AccessCatalogFields with the Default Values

Order	Visible	Column-name	Label
0	True	Application Name	Application Name
1	True	AccessName	Access
2	True	Description	Info

Configuring the Confirmation Popup

Requesters are shown a popup to confirm their selection when they add an access level to their request. The popup confirms that an access level has been added. You can decide to show or hide the popup by configuring the **ACCESSCATALOGSHOWCONFIRMATIONPOPUP** global option.

Constraining the Access Levels Visible to Requesters

Depending on the function of the requesters who log in, you can restrict which access levels they can select on the **ACCESS CATALOG** window. For example, if Resource Owners log in to the Access Request Manager and select a recipient, they can select access levels only for resources they own.

The following global options determine the restrictions on the selection of access levels:

- **ACCESSCATALOGDEFAULT RESTRICTIONMACRO** - References the `Get AccessCatalog Default Restriction` custom macro that implements restrictions on a requester logging in with an enterprise-specific function, such as a Project Manager.
- **ACCESSCATALOGINDIVIDUAL CONTRIBUTORRESTRICTIONMACRO** - References the `Get AccessCatalog Individual Contributor Restriction` custom macro that implements restrictions on a requester logging in as an Individual Contributor.
- **ACCESSCATALOGMANAGERRESTRICTIONMACRO** - References the `Get AccessCatalog Manager Restriction` custom macro that implements restrictions on a requester logging in as a Business Manager.
- **ACCESSCATALOGRESOURCEOWNERRESTRICTIONMACRO** - References the `Get AccessCatalog Resource Owner Restriction` custom macro that implements restrictions on a requester logging in as a Resource Owner.

Custom Macros to Implement for Adding Access Levels

The Access Request Manager provides the custom macros described in Table 13 to implement restrictions against the access levels displayed on the **ACCESS CATALOG** window. The restriction defines which access levels requesters can see, based on their function, during the request workflow.

Table 13: Custom Macros that Implement Search Restrictions

Custom Macro	Default Restriction
Get AccessCatalog Default Restriction	<p>A user with enterprise-specific function, such as a Project Manager sees all access levels for all applications by default.</p> <p>Implement a new constraint, such as allowing a Project Manager to see access levels associated with their project.</p>
Get AccessCatalog Individual Contributor Restriction	<p>An Individual Contributor sees all access levels for all applications by default.</p> <p>Implement a new constraint, such as allowing Individual Contributors to see access levels relevant to their department.</p>
Get AccessCatalog Manager Restriction	<p>Business Managers see all access levels for all applications by default.</p> <p>Implement a new constraint, for example, allow Business Managers to see access levels relevant to their department.</p>
Get AccessCatalog Resource Owner Restriction	<p>Resource Owners see all access levels for all applications owned by them by default.</p> <p>Implement new constraints, for example:</p> <ul style="list-style-type: none"> • To allow the Resource Owner to see all access levels. • To allow the Resource Owner to see all access levels for applications they own, including all access levels associated with their location.

Verifying Access Levels

This section describes how you can configure the **VERIFY** window for requesters to verify access levels. You can configure the following items on the **VERIFY** window:

- The popup that displays the user access information.


Requesters can see which recipients have the selected access level by selecting the User icon , and seeing the information in the **USER ACCESS** popup. You can specify the fields that appear on the popup by configuring the **USERACCESSFIELDS** global option. The fields are from the Profile table.

Table 14 shows the default values for **USERACCESSFIELDS**

Table 14: UserAccessFields with the Default Values

Order	Visible	Column-name	Label	Control	Required
0	True	FirstName	First Name	Text	True
1	True	LastName	Last Name	Text	True
2	True	Department	Department	Text	True

Chapter 5: Configuring the Approval Workflow

This chapter describes how to use the Administration Interface to configure the approval workflow, and includes the following sections:

- [*“Adding Second-Level Approvers” on page 62*](#)
- [*“Approving the Requests” on page 64*](#)

Before you configure the **REQUEST APPROVAL** window, review the section [*“Using the Global Configuration Manager” on page 21*](#) that describes the global options used in this chapter and how to edit them.

Adding Second-Level Approvers

Requests submitted by the requesters in the request workflow are sent to approvers for approval. Business Managers of the recipients are by default the first-level approvers. The second-level approvers are then notified about the request for their approval.

You can configure the second-level approvers through the **APPLICATION/ACCESS MANAGER**.

To add second-level approvers, follow these steps:

Note: Second-level approvers are configured at the access level. You first add the access levels for which you want to add second-level approvers. To add the access levels, refer to [“Adding Access Levels” on page 50](#).


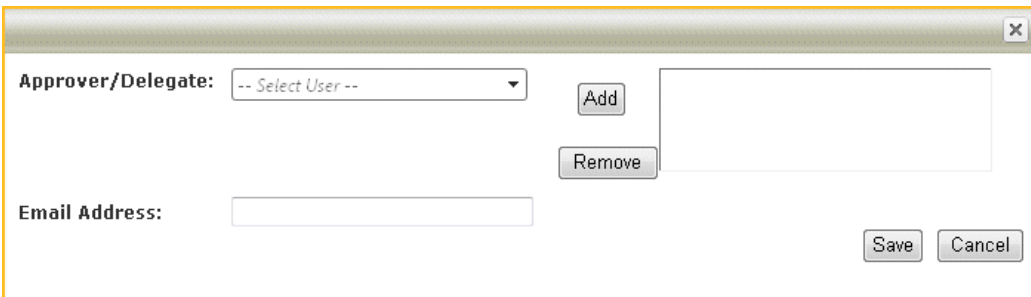
1. Select **APPLICATION/ACCESSES** from the top-level menu. The **APPLICATION/ACCESS MANAGER** appears.
2. Click the Edit icon  to edit the application. A window appears with the application and the related access levels displayed in a grid.
3. Click **SELECT** for the access level to which you want to add an approver. The window expands with an option to add one or more second-level approvers.
4. Select **ADD APPROVER**. A new window appears for you to enter the approver details, as shown in [Figure 29](#).

Figure 29: Add Approver



Configure the following fields:

APPROVER/DELEGATE: Add one or more approvers by clicking **ADD**. The drop-down list supports the type ahead feature, so you do not need to scroll through the list to find the name you need.



The information for the drop-down list is retrieved from the Profile table.

EMAIL ADDRESS: Enter the email address of the approver. Since you can add only one email address, use a distribution list if you want to notify multiple approvers.

5. Click **SAVE** to add the approver.

On closing the window, the approver name you added appears in the **SECONDARY APPROVER/USER ACCESS OWNER DELEGATE** window, as shown in [Figure 30](#).

Figure 30: List of Approvers Added

Approvers			
AD Login(s)	Distribution List	Edit	Delete
probinson	approvers@company.com		

Approving the Requests

Approvers can view all the pending requests on the **REQUEST APPROVAL** window. Any bulk request the requester submits is displayed as individual requests with one request for each recipient. For example, if a Business Manager selects three recipients for an access level in a request, the approver sees three individual requests.

In the default approval process, the recipient's Business Manager approves first. The request is then sent in parallel to all second-level approvers. If there are multiple second-level approvers, the first one to act approves or denies the request.

If the requester is the recipient's Business Manager, the request is considered approved by the Business Manager. Business Managers do not have to approve requests they submitted for their direct reports. Similarly, if Resource Owners submit a request, they do not have to approve that request.

You can configure the following items on the **REQUEST APPROVAL** window:

- Fields for the grid that shows the pending requests.
- The fields and action buttons on the **REQUEST DETAILS** window.

Setting Up Fields for Pending Requests


The approver can see the pending requests in the **APPROVAL REQUESTS** grid. Specify the fields for this grid by configuring the **APPROVALQUEUEDISPLAYCOLUMNS** global option. The fields are from the Request table.

Table 15 shows the default values for **APPROVALQUEUEDISPLAYCOLUMNS**.

Table 15: ApprovalQueueDisplayColumns Default Values

Column-name	Order	Visible	Label
RequestID	0	True	Request Number
FirstName	1	True	Prov.'s First Name
LastName	2	True	Prov.'s Last name
Provisioner	3	True	Requester

Setting Up Fields for Request Details

The approver can see additional information about a particular request by selecting the Status icon . The **REQUEST DETAILS** window appears with information about the access level, the requester and the recipient. The approver can approve or deny the access level. You can configure the fields and the action buttons that appear on this window.

Setting Up Fields To View Requester Details

The approver can see details about the requester in the **REQUEST** grid. The displayed information is from the Request Detail table. To specify the fields from the Request Detail table, use the **EDIT COMPLEX VALUES** button for the **APPROVALREQUESTDETAILFIELDS** global option.

Table 16 shows the default values for **APPROVALREQUESTDETAILFIELDS**.

Table 16: ApprovalRequestDetailFields Default Values

Column-name	Order	Visible	Label
RequestID	0	True	Request Number
UserType	1	True	User Type
Request Date	2	True	Date Submitted

Setting Up Fields to View Recipient Details

The approver can see the recipient information in the **EMPLOYEE** grid. The displayed information is from the Profile table. To specify the fields from the Profile table, use the **EDIT COMPLEX VALUES** button for the **APPROVALPROFILEDISPLAYFIELDS** global option.

Table 17 shows the default values for **APPROVALPROFILEDISPLAYFIELDS**.

Table 17: ApprovalProfileDisplayFields Default Values

Column-name	Order	Visible	Label
ProfileUID	0	True	Employee ID
FirstName	1	True	First Name
LastName	2	True	LastName
Department	3	True	Department

Setting Up Fields to View Access Levels

The approver can see the access level information in the **ACCESS** grid. The displayed information is from the RequestApprovals table. To specify the fields from the RequestApprovals table, use the **EDIT COMPLEX VALUES** button for the **APPROVALACCESSDISPLAYFIELDS** global option.

Table 18 shows the default values for **APPROVALACCESSDISPLAYFIELDS**.

Table 18: ApprovalAccessDisplayFields Default Values

Column-name	Order	Visible	Label
AccessID	0	True	Request Number
Status	1	True	Status
Application	2	True	Application
Comments	3	True	Comments

Configuring the Approve and Deny Action Buttons

The approver can approve or deny a request by clicking the action buttons in the **ACCESS** grid. The approver checks the checkbox next to the access level before approving or denying the access level.

To set up the **APPROVE** button, configure the **APPROVALACTIONAPPROVE** global option. Table 19 shows the default values for **APPROVALACTIONAPPROVE**.

Table 19: ApprovalActionApprove Default Values

Column-name	Label	Require-comment
Approve	Approve	False

To set up the **DENY** button, configure the **APPROVALACTIONDENY** global option. Table 20 shows the default values for **APPROVALACTIONDENY**.

Table 20: ApprovalActionDeny Default Values

Column-name	Label	Require-comment
Deny	Deny	True

If the require-comment field is set to true, the approver is required to provide a comment. If the field is set to false, the comment is optional.

Note: The column-name in the XML strings for **APPROVALACTIONAPPROVE** and **APPROVALACTIONDENY** identifies an action.

Displaying the Checkbox to Enable Collective Approval

You can enable the approver to do a bulk approval. With a single click, the approver can select all the displayed access levels for either approval or denial. This checkbox is configured through the **APPROVALBULKACTIONAVAILABLE** option by setting the value for **CONFIG VALUE** to **TRUE**. If **CONFIG VALUE** is set to **FALSE**, the approver must select each access level individually for approving or denying.

Note: The approver can either do a collective approval or individual approval of requests with this global option configured.

Note: The **SELECT ALL** checkbox applies to the displayed items. If there are multiple windows of access levels, the approver must act on all the windows.

Displaying the Checkbox to Enable Only Collective Approval

The approver can select the **SELECT ALL** checkbox to do only collective approvals. In this case, the option to approve individual requests is not available.

To require the approver to do only collective approvals, configure the **APPROVALBULKACTIONONLY** global option by specifying the **CONFIG VALUE** as **TRUE**.

Note: The approver does not see the individual checkboxes to individually approve requests if this global option is configured.

Chapter 6: Setting Up Email Notifications

This chapter describes how to configure email notifications that are sent when a request is submitted for approval, using the **EMAIL TEMPLATES MANAGER**.

Email notifications are sent to all the relevant users: the requesters, the Business Managers (first-level approvers), and the second-level approvers who participate in the approval of a request.

Note: The Business Managers by default are the first-level approvers.

The **EMAIL TEMPLATES MANAGER** offers default email templates, as shown in Table 21 .

Table 21: The Default Email Templates for Notification

Default Email Type	Sent To	Notification is Sent
AccessApproval	Requesters, Business Managers	<p>If an access level is approved, notification is sent with information about the access level and the approver.</p> <p>Note: Notifications are sent for every access level in a request. For example, if a requester submits a request with three access levels and an approver approves two of them, notifications are sent for each approved access level.</p>
AccessDenial	Requesters, Business Managers	<p>If an access level is denied, notification is sent with information about the access level and the approver.</p> <p>Note: Notifications are sent for every access level in a request. For example, if a requester submits a request with three access levels and an approver denies two, notifications are sent for each denied access level.</p>

Table 21: The Default Email Templates for Notification

















Default Email Type	Sent To	Notification is Sent
ManagerApproval	Business Manager (first-level approver)	<p>If the requester is other than the Business Manager of the recipient, then the Business Manager receives notification for first-level approval.</p> <p>Note: Notification is sent for every single recipient selected in a request. For example, Business Managers receive two notifications if two of their direct reports are selected in a single request.</p> <p>If Business Managers submit requests for their direct reports, the first-level approval is complete.</p>
RequestSubmission	Requester	The requester is notified when the request is submitted.
SecondaryApproval	Second-level approvers	Once the first-level approval is complete, notification is then sent to all second-level approvers.


Editing a Default Email Template

To customize a default email template:

1. Click **CONFIGURATION** and select **EMAIL TEMPLATE CONFIGURATION** from the drop-down list. The **EMAIL TEMPLATES MANAGER** appears as shown in [Figure 31](#).

Figure 31: Email Templates Manager

Email Templates Manager			
Email Type	Subject	Edit	Delete
AccessApproval	Access Approved for Access - %AcceesName% for %FirstName% %LastName%		
AccessDenial	Access Denied for Request# %RequestID%		
LeaverPhysicalAsset	FYI - Account Deletion of all System Access for %FullName% %ADLogin%		
LeaverRequest	Attention - Account(s) Disabled: %RequestID% %FullName% %ADLogin%		
LTADisableRequest	Attention - Account(s) temporarily Disabled: %RequestID% %FullName% %ADLogin%		
ManagerApproval	ACTION REQUIRED - Review Needed for Request: %RequestID% %FirstName% %LastName% %ADLogin%		
RequestSubmission	Request Submitted: %RequestID% %FirstName% %LastName%		
SecondaryApproval	ACTION REQUIRED - Review Needed for Request: %RequestID% %FirstName% %LastName% %ADLogin%		

 Add Template



- Click the Edit icon  to edit the subject or the body text of the email template you selected. See [Figure 32](#).

Figure 32: Add New Email Template

Name:




Subject:

Body:

Font Name Size **B** *I* U 

Your request for Access - %AcceesName% has been approved by %FirstName% %LastName%.

Thank You

 Design  HTML  Preview

Customize the following fields:

SUBJECT: Enter the topic of the email you want to display to the requester or the approver.

BODY: Enter the message you want to send as a notification. The email template macros specified in the %<macros may be used>% retrieve information from the Profile table.

3. Click **Save** to save the message or **CANCEL** to reset to the previous message.

Chapter 7: Managing Access to the Access Request Manager Web Pages

This chapter describes how to configure user access to menu items and to specific Access Requester Manager web pages, using the **SECURITY ADMINISTRATOR**.

The Access Request Manager implements the following to enable you to provide users access to the web pages:

- Communities
- Entitlements
- Functions (introduced in [“About the Access Request Manager” on page 5](#)).

This chapter includes the following sections:

- [“Community” on page 74](#)
- [“Entitlements” on page 75](#)
- [“Functions” on page 79](#)

Community

A community is a set of users that have a common set of privileges. The Access Request Manager supports the following communities:

- Everyone
- Business Managers
- Resource Owners
- Access Approvers
- ARM Admins

When users authenticate into the Access Assurance Portal, a macro determines the community to which users belong by matching the community to their Active Directory group membership. To match a community to an Active Directory group, you must create a corresponding group with the same name in the Active Directory Domain. For more information about configuring Active Directory groups, refer to the section [“Installing and Configuring the Access Request Manager” on page 14](#).

Table 22 lists the community and the corresponding AD group.

Table 22: Communities and their AD Groups

Community	AD Group
Everyone	All users in Active Directory
Business Managers	Business Managers
Resource Owners	Resource Owners
Access Approvers	Access Approvers
ARM Admins	ARM Admins

Entitlements

Entitlements determine the menu items that appear on the Access Assurance Portal and the web pages displayed to the user.

The Access Request Manager supports the following entitlements:

- Basic Access
- Business Manager
- Resource Owner
- Access Approver
- ARM Admin

An entitlement consists of zero or more communities. For example, the Business Manager entitlement consists of the Business Managers community. At installation, the Access Request Manager maps the default entitlements to the menu items in the Portal Menu table.

Table 23 lists the default for entitlements, the related communities, AD Groups, and the associated menu items.

Table 23: Entitlements with the Related Communities, AD Groups and Menu Items

Entitlement	Community	AD Group	Menu Item
Basic Access	Everyone	All users in Active Directory	ACCESS REQUEST, VIEW REQUEST
Business Manager	Business Managers	Business Managers	REQUEST APPROVAL
Resource Owner	Resource Owners	Resource Owners	None
Access Approver	Access Approvers	Access Approvers	REQUEST APPROVAL
ARM Admin	ARM Admins	ARM Admins	APPLICATION/ ACCESSES, CONFIGURATION, SECURITY ADMIN, PRIORITY DISABLE

For example, a user who belongs to the Business Managers AD group is in the Business Managers community. Since the Business Managers community resides in the Business Manager entitlement, all menu items associated with this entitlement are displayed to the user.

To change the menu items associated with an entitlement, modify the Portal Menu table entries. For example, if you want to:

- Prevent Individual Contributors from requesting access, but continue to allow Business Managers to request access for their direct reports, and
- Allow Resource Owners to request access to their owned resources, then follow these steps:
 - a. Delete the Basic Entitlement from the Portal Menu table.

- b. Add the **ACCESS REQUEST** and **VIEW REQUEST** menu items to the Portal Menu table for the Business Manager and Resource Owner entitlements.

Securing Access to Web Pages

Since the entitlements also determine the web pages displayed to the user, follow these steps to give access to specific web pages:

Note: The default is no access.

Select **SECURITY ADMIN** from the top-level menu. The **SECURITY ADMINISTRATOR** appears as shown in [Figure 33](#).

Figure 33: Managing Access with the Security Administrator

The screenshot shows the Security Administrator interface with two main sections: Entitlements and Security Pages.

Entitlements Table:

Entitlement	Alias	Edit	Delete
Basic Access	Basic Access		
Resource Owner	Resource Owners		
Access Approver	Access Approvers		
ARM Admin	ARM Admins		
Business Manager	Business Managers		

Buttons: + Add Entitlement, Refresh

Security Pages Table:

Page	Entitlement	Edit	Delete
accessrequest.aspx	Basic Access		
viewrequest.aspx	Basic Access		
approvalqueue.aspx	Access Approver		
rolemanager.aspx	ARM Admin		
disableuser.aspx	ARM Admin		
globalconfigurationmanager.aspx	ARM Admin		
manageapplications.aspx	ARM Admin		

Buttons: + Add Page, Refresh

Click **ADD ENTITLEMENT**. A window appears for you to add the entitlement and an alias, as shown in [Figure 34](#).

Figure 34: Add Entitlement

The screenshot shows the "Add Entitlement" dialog box within the Security Administrator interface. It contains two text input fields and two buttons.

Fields:

- Entitlement:
- Alias:

Buttons: Insert, Cancel

Enter the **ENTITLEMENT** into textbox, such as Business Manager. Enter an **ALIAS**, such as Business Managers. Click **INSERT**.

Next, click **ADD PAGE** to assign a web page to the entitlement you just added. Enter the web page in the **PAGE** field to which you want to enable access, as shown in [Figure 35](#).

Figure 35: Add Web Page

The screenshot shows a window titled "Security Pages". Inside, there is a table with two columns: "Page" and "Entitlement". Below the table, there are input fields for "Page:" and "Entitlement:". The "Entitlement:" field has a dropdown menu currently showing "-- Select Entitlement -". To the right of the input fields are four buttons: "Edit", "Delete", "Insert", and "Cancel".

For example, add `accessrequest.aspx`. Select the **ENTITLEMENT** alias from the drop-down list, for example Business Managers. Select **INSERT** to add the web page to the **SECURITY PAGES**. Only those users who belong to the Business Managers community can see the page you added.

Entitlement and Web Page Pairs in the Access Request Manager

Table 24 lists the default entitlement and web page pairs in the Access Request Manager.

Table 24: Web Pages and the Entitlements

Entitlement	Web page
Basic Access	<code>accessrequest.aspx</code>
Basic Access	<code>viewreqeust.aspx</code>
Access Approver	<code>approvalqueue.aspx</code>
ARM Admin	<code>rolemanager.aspx</code>
ARM Admin	<code>disableuser.aspx</code>
ARM Admin	<code>globalconfigurationmanager.aspx</code>
ARM Admin	<code>manageapplications.aspx</code>
ARM Admin	<code>editapplication.aspx</code>
ARM Admin	<code>manageemailtemplates.aspx</code>
ARM Admin	<code>picklistadmin.aspx</code>
ARM Admin	<code>admin/viewrequest.aspx</code>
ARM Admin	<code>securityadmin.aspx</code>
ARM Admin	<code>editrole.aspx</code>
ARM Admin	<code>roledetails.aspx</code>
ARM Admin	<code>editemailtemplate.aspx</code>
Business Manager	<code>approvalqueue.aspx</code>

Adding Web Pages for a New Entitlement

If, for example, you want to add a new Active Directory group, such as HR Managers and provide access to the **PRIORITY DISABLE** page so they can disable access for a terminated user, follow these steps:

1. Create HR Managers in the Active Directory domain.
2. Add the HR Managers AD group to the AD account of all HR Managers who you want to allow to use the Priority Disable web page.
3. Create an HR Managers community and add the HR Managers AD group to it.
4. Create an HR Manager entitlement and add the HR Managers community to it.
5. Add the HR Manager entitlement to the Portal Menu table and provide access to the Portal Disable menu item.
6. Follow the steps in [“Securing Access to Web Pages” on page 76](#) to add the web page disableuser.aspx for the HR Manager entitlement.

Changing the Default Landing Page of the Portal

Any user who authenticates into the Access Assurance Portal sees the default landing page with the menu item **PORTAL HOME**. To change the default landing page, follow these steps:

1. Go to the Portal Menu table found in the Transaction Repository database. The MetricRepositoryDefault connection string in the Analytics\AccessCertification\Web.Config file points to this database.
2. Edit the entitlement for which you want to change the default landing page by modifying one or more of the following fields:
 - Caption:** The label for the top-level menu item.
 - Entitlement:** The entitlement that has access to the relevant menu item.
 - ListOrder:** Dictates the order of the menu items. The Listorder field with the lowest value will display as the first left-most menu item. Accepts an integer value starting from 1.
 - Default:** True or False. A value of true displays the menu item with the related web page as the default landing page. If there are multiple records with the Default field set to true, the lowest ListOrder menu item with the Default field as true will appear as the default landing page.

The Business Manager entitlement includes all users in the Business Managers community who see the default landing page with the menu item **PORTAL HOME**. For example, if you want to change the default landing page for the Business Manager entitlement to see **ACCESS REQUEST**, follow these steps:

1. Set the Default field to true if it is set to false for the record with fields Caption=Access Request and Entitlement=Basic Access.
2. Set Default to false for the record with fields Caption=Portal Home and Entitlement=Basic Access.
3. The **ACCESS REQUEST** menu item is displayed with the Access Request window as the default to a Business Manager who authenticates into the Portal.

Functions

The Access Request Manager supports the following functions:

- Individual Contributors
- Business Managers
- Resource Owners

The Functions determine:

- The recipients that the requesters can search on the **USER DETAIL** window.
- The access levels the requesters can request on the **ACCESS CATALOG** window.

Table 25 lists the functions and the access levels they can see depending on whom they select as recipients.

Table 25: Functions and the Access Levels Available

Functions			Providing Access For	Access Levels Available
Individual Contributor	Business Manager	Resource Owner		
Yes			Self	All
Yes		Yes	Self	All
Yes		Yes	Any recipient other than Self	Owned access levels
	Yes		Self	All
	Yes		Direct Reports	All
	Yes	Yes	Self	All
	Yes	Yes	Direct Reports	All
	Yes	Yes	Any recipient other than Self and Direct Reports	Owned access levels

Chapter 8: Customizing the Access Request Manager User Interface

This chapter describes how to customize the Access Request Manager user interface using the `AccessReqMgrResources.resx` resource file. This resource file is found in the `Analytics\App_GlobalResources` folder. Use any text editor to edit the resource file.

The resource file enables you to customize the text displayed for buttons, tabs, and dialog boxes for a specific language or culture. For example, to customize the text **Denotes Required Field**, which is displayed on the **USER DETAIL** window, edit the `<name>/<value>` pair of the XML data tag in the resource file:

```
<data name="lblRequiredField" xml:space="preserve">
    <value>Denotes Required Field</value>
    <comment>Required field indicator label</comment>
</data>
```

Customize the `<value>` tag to display new text:

```
<data name="lblRequiredField" xml:space="preserve">
    <value>You must enter these fields.</value>
    <comment>Required field indicator label</comment>
</data>
```

The **USER DETAIL** window shows **"You must enter these fields."** as the new text.

Displayed Text in the Resource File

Table 26 lists the displayed text available to you for editing in the resource file.

Table 26: Strings in the Resource File

Name	Displayed Text	Type	Location
ACCESS_CATALOG_ACCESS_ADDED	This access has been added to your request.	Message shown when an access level is added.	ACCESS CATALOG

Table 26: Strings in the Resource File

Name	Displayed Text	Type	Location
ACCESS_CATALOG_ACCESS_REMOVED	You can only request access levels for resources owned by you. Since you have selected recipients who are not your direct reports, some access levels have been removed.	Message displayed if the logged in user is a Business Manager, but acting as a Resource Owner.	ACCESS CATALOG
ACCESS_CATALOG_FILTER_RESULTS	Filter Results	Label for the grid that displays the filtered access levels.	ACCESS CATALOG
ACCESS_CATALOG_PRIMARY_FILTER	Filter By:	Label for the primary drop-down list	ACCESS CATALOG
ACCESS_CATALOG_PRIMARY_FILTER_ERROR	Primary Filter could not be loaded. Please check logs for more information.	Error message displayed when the primary drop-down list does not appear.	ACCESS CATALOG
ADD_ACCESS_ATTRIBUTE_COULD_NOT_BE_LOADED	Add Access Attribute could not be loaded. Please check logs for more information.	Error message displayed when the popup does not appear to enter configuration information.	ACCESS CATALOG VERIFY
ADD_ACCESS_ATTRIBUTE_COULD_NOT_SAVE_PROFILE	Access Attribute information could not be saved. Please check logs for more information.	Error message displayed if the configuration information could not be saved.	ACCESS CATALOG VERIFY
ADD_NEW_ASSIGNEE_CONFIG_XML_ERROR	Add New Assignee Configuration Settings XML could not be processed. Please check logs for more information.	Error message displayed if the AddNewAssigneeFields global option could not be processed properly.	USER DETAIL
ADD_NEW_ASSIGNEE_COULD_NOT_SAVE_PROFILE	Assignee information could not be saved. Please check logs for more information.	Error message displayed if the new recipient profile information added by the requester could not be saved.	USER DETAIL
ADD_NEW_ASSIGNEE_DUPLICATE_PROFILE	A Profile already exists with the given unique identifier.	Error message displayed if the ProfileUID of the new recipient added by the requester already exists.	USER DETAIL

Table 26: Strings in the Resource File

Name	Displayed Text	Type	Location
ADD_NEW_ASSIGNEE_PANEL_NOT_LOADED	Add New Assignee Panel could not be loaded. Please check logs for more information.	Error message displayed if the ADD NEW grid to add a new recipient does not appear.	USER DETAIL
ADV_SEARCH_CONFIG_XML_ERROR	Advanced Search Configuration Settings XML could not be processed. Please check logs for more information.	Error message displayed if the MultiUserSearchOption global option could not be processed properly.	USER DETAIL
ADV_SEARCH_PANEL_NOT_LOADED	Advanced Search Panel could not be loaded. Please check logs for more information.	Error message displayed if the SEARCH WITH MORE OPTIONS grid is not displayed correctly.	USER DETAIL
ADD_NEW_PROFILEUID_MUST_EXIST	The Add New Configuration Settings XML is missing the ProfileUID field. To add a new recipient, this field must exist in the Configuration XML.	Message displayed if the AddNewAssigneeFields global option does not contain the ProfileUID field while the requester tries to add a new recipient.	USER DETAIL
btnSearchEmployee	Go	Button Label	USER DETAIL
BUTTON_ACTION	Action	Column Header	VERIFY
BUTTON_ADD	Add	Column Header	ACCESS CATALOG
BUTTON_BACK	Back	Button Label	As Needed
BUTTON_CONFIGURE	Configure	Column Header	VERIFY
BUTTON_INFO	Info	Column Header	ACCESS CATALOG
BUTTON_NEXT	Next	Button Label	As Needed
BUTTON_USERS	Users	Column Header	VERIFY
DROPDOWN_SELECT_TEXT	-----Select-----	Text displayed in a drop-down list	As needed
lblAssigneeType	Providing Access For	Label for the Drop-down list to select a recipient category.	USER DETAIL
lblProvisioner	Acting As	Label to describe who the requester is "acting as."	USER DETAIL

Table 26: Strings in the Resource File

Name	Displayed Text	Type	Location
lblRequiredField	*Denotes Required Field	Help information	USER DETAIL
NO_ASSIGNEES_SELECTED	No assignees were selected. Please select one or more assignees in order to proceed.	Message displayed if the requester does not select any recipients.	USER DETAIL
PENDING_APPROVAL_TEXT	Requests Pending Approval	Label for the grid that shows the pending requests	REQUEST APPROVAL
rbAddNew	Add New	Label for the radio button.	USER DETAIL
rbMoreSearch	More Search Options	Label for the radio button	USER DETAIL
REQD_VALIDATION	Please provide data for required fields	Message displayed to a user to provide required information	As Needed
RESULTS_FOUND	Found	Text displayed next to the DIRECT REPORTS checkbox in the SEARCH WITH MORE OPTIONS grid.	USER DETAIL
SELECTED_ASSIGNEES	Selected Recipients	Label for the grid that displays the selected recipients.	ACCESS CATALOG VERIFY
tabAccessCatalog	Access Catalog	Tab Label	ACCESS CATALOG
tabUserDetail	User Detail	Tab Label	USER DETAIL
tabVerify	Verify	Tab Label	VERIFY
USER_DETAIL_ACTING_AS_INFO	Select Myself	Help text displayed to the user for the ACTING AS drop-down list.	USER DETAIL
USER_DETAIL_SEARCH_INFO	Find access recipients	Help text displayed to the user for the search options.	USER DETAIL
USERDETAIL_ASSIGNEE_TYPE_ERROR	Assignees are not loaded. Please check logs for more information.	Error message displayed if the PROVIDING ACCESS FOR drop-down list does not display the categories correctly.	USER DETAIL

Table 26: Strings in the Resource File

Name	Displayed Text	Type	Location
USER_DETAIL_SINGLE_USER_SEARCH_MULTIPLE_RESULTS	More than one record was found for your search criteria. Please use the More Search Options to search for multiple users.	Message displayed if more than one record is found for a recipient when a requester searches on a unique field for a single recipient.	USER DETAIL
USERPROFILEDETAIL_NO_SEARCH_RESULTS	No matches found	Message displayed when a requester searches for a recipient, and no recipients are found.	USER DETAIL
VERIFY_ACCESS_ATTRIBUTES_ERROR	An error occurred while saving the request. Please check logs for more information.	Error message displayed if a request submitted by the requester was not saved.	VERIFY
VERIFY_ACCESS_ATTRIBUTES_MISSING	Additional access level information is required. Please click on the tools icon to provide this information.	Message displayed if the requester does not provide the required configuration information for one or more access levels.	VERIFY
VERIFY_ACCESS_REQUEST_ACTION_ADDED	Added	Text displayed in the Action column if an access level is added in a request.	VERIFY
VERIFY_ACCESS_REQUEST_ACTION_CURRENT	Current	Text displayed in the Action column for an access level already provisioned earlier through the Access Request Manager.	VERIFY
VERIFY_ACCESS_REQUEST_ACTION_REMOVED	Removed	Text displayed in the Action column if an access level is removed.	VERIFY
VERIFY_ACCESS_REQUEST_ERROR	Could not retrieve selected Access. Please check logs for more information.	Error message displayed if the grid with the access level information does not appear.	VERIFY
VERIFY_ACCESS_REQUEST_SUBMITTED	The request has been submitted.	Confirmation message displayed when a request is successfully submitted.	VERIFY

Chapter 9: Disabling Access with Priority Disable

This chapter describes how to immediately disable access for users who are being terminated.

You can disable access for the user by selecting **PRIORITY DISABLE** from the top-level menu. The **DISABLE USER** window appears, as shown in [Figure 36](#).

Figure 36: Disabling Access with Priority Disable

Enter the Active Directory user name of the user in to the **AD LOGIN** textbox and select **VALIDATE**. The **USER PROFILE** and **CURRENT ACCESS** grids are populated with the profile information and all the access levels the user may have.

Enter any comments you may have, and select the checkbox if you want to **SUBMIT**.

Index

A

about
 Access Request Manager 5
 Access Assurance Portal 5
 authenticate 18
 Access Assurance Suite 5
 Access Keys 6
 access level 9, 47
 add 50
 access request workflow 7
 Active Directory groups 14
 add
 access level 50
 application 48
 roles 55
 Administration Interface 18
 Administration Interface, menu items 18
 administrator 5
 Application/Access Manager 19
 approval workflow 7
 approver 7
 first-level 62, 69
 second-level 62, 69

B

bulk request 11
 Business Manager 5

C

Community 73, 74
 connection string 14
 Courion notification service 14, 16
 Courion request service 14, 16
 custom macros 45, 46, 59

E

edit
 email template 70
 email template
 edit 70
 Email Templates Manager 19
 Entitlement 9, 73, 75

F

first-level approver 62, 69
 Function 5, 73, 79

G

Global Configuration Manager 19, 21
 global options 21
 defaults 21
 edit 29

I

Individual Contributor 5
 installing 14

L

landing page 78

P

Pick List Admin 19, 34
 picklists
 add 36
 defaults 35
 values 35
 primary drop-down list 47

R

recipient 7
 requester 7
 resource file 81
 Resource Owner 5
 restrictions 45
 Role Manager 19
 roles
 add 55

S

secondary drop-down list 47
 second-level approver 62, 69
 Security Admin 19
 SQL scripts 14, 15

X

XML data tag 81

